Supplemento ordinario alla "Gazzetta Ufficiale,, n. 218 del 19 settembre 2005 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Lunedì, 19 settembre 2005** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081

N. 155

MINISTERO DELL'INTERNO

DECRETO 2 agosto 2005.

Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE, in attuazione del comma 2 dell'articolo 7-*vicies ter* della legge 31 marzo 2005, n. 43.

SOMMARIO

MINISTERO DELL'INTERNO

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'INTERNO

DECRETO 2 agosto 2005.

Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE, in attuazione del comma 2 dell'articolo 7-*vicies ter* della legge 31 marzo 2005, n. 43.

IL MINISTRO DELL'INTERNO

Visti il regio decreto 18 giugno 1931, n. 773 ed il regio decreto 6 maggio 1940, n. 635;

Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

Visto il decreto del Ministro dell'interno in data 19 luglio 2000 concernente regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto-legge 23 gennaio 2000, n. 10;

Visto il decreto legislativo 30 giugno 2003, n. 196;

Visto il decreto-legge 7 marzo 2005, n. 82;

Vista la legge 31 marzo 2005, n. 43;

Vista la legge 31 maggio 2005, n. 88;

Visto il comma 2, art. 7-*vicies ter* della legge 31 marzo 2005, n. 43, che stabilisce che i comuni che non vi abbiano ancora ottemperato provvedano entro il 31 ottobre 2005 alla predisposizione dei necessari collegamenti all'Indice Nazionale delle Anagrafi (INA) presso il Centro Nazionale per i Servizi Demografici (C.N.S.D.) ed alla redazione del piano di sicurezza per la gestione delle postazioni di emissione secondo le regole tecniche fornite dal Ministero dell'Interno;

Considerato che il Piano di sicurezza comunale per la carta di identità elettronica «Piano di sicurezza comunale per la carta di identità elettronica: linee guida e metodologia per la redazione del piano», è stato sperimentato sul campo presso 3 comuni rappresentativi delle tipologie di grande, di medio e di piccolo Comune;

Decreta:

Capo I

PRINCIPI GENERALI

Art. 1.

Definizioni

1. Ai sensi del presente decreto si intende:

a) per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437;

b) per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;

c) per «dati»: i dati identificativi della persona di cui all'art. 1, comma 1, lettera *d)* e gli altri elementi di cui all'art. 3, comma 1, lettere da *b)* ad *h),* del decreto del Presidente del Consiglio dei Ministri;

d) per «S.S.C.E.»: il Sistema di sicurezza del circuito di emissione dei documenti di identità elettronica;

e) per «C.N.S.D.»: il Centro Nazionale dei Servizi Demografici del Ministero dell'Interno costituito con il decreto del Ministro dell'interno del 23 aprile 2002;

f) per «I.N.A.»: l'Indice Nazionale delle Anagrafi istituito con legge 28 febbraio 2001, n. 26, sostituita dalla legge 31 maggio 2005, n. 88, per la fornitura dei servizi di convalida anagrafica durante l'emissione e l'uso del documento;

g) per Backbone C.N.S.D.: la dorsale di sicurezza e certificazione del C.N.S.D. per l'accesso ai servizi applicativi del C.N.S.D.;

h) per «Porta di accesso ai domini applicativi del C.N.S.D.»: la Porta di accesso, attraverso il Backbone C.N.S.D., ai servizi del C.N.S.D. secondo standard «busta di e-gov» di SPC;

i) per «Porta di accesso»: una «Porta di accesso ai domini applicativi del C.N.S.D.»;

l) per «Porta di accesso del Comune»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso il comune;

m) per «Porta di accesso della Prefettura-UTG»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso la prefettura-UTG;

n) per «Porta di accesso del centro di allestimento periferico»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso un centro di allestimento periferico;

o) per «Busta di e-gov»: il formato comune di interscambio tra porte di dominio di enti diversi;

p) per «sito»: il sito Web della Direzione Centrale per i Servizi Demografici, accedibile all'indirizzo internet www.servizidemografici.interno.it;

q) per «quantità di sicurezza, certificazione ed attivazione»: le credenziali digitali e i software di sicurezza, monitoraggio e allarmi forniti dal Ministero dell'interno;

r) per SPC: il Sistema pubblico di connettività di cui al decreto legislativo n. 42 del 28 febbraio 2005;

s) per «domini applicativi»: i domini applicativi del C.N.S.D., ovvero l'insieme dei servizi applicativi riferiti ad un'area (INA, AIRE, Stato civile ...);

t) per «servizi applicativi»: i servizi applicativi dei singoli domini applicativi del C.N.S.D.;

u) per «Protocollo XML-Soap»: il protocollo di trasporto della «busta di e-gov del C.N.S.D.» che uniforma i messaggi scambiati con la Porta di accesso;

v) per busta di e-gov del C.N.S.D.: la busta di e-gov relativa ai domini applicativi del C.N.S.D.;

aa) per «Protocollo post http XML»: la trasmissione di un evento in formato XML alla Porta di accesso;

ab) per «C.I.E.»: Carta di identità elettronica;

ac) per «AIRE»: Anagrafe italiani residenti all'estero;

ad) per allegato A si intende il «Piano di sicurezza comunale per la carta di identità elettronica: linee guida e metodologia per la redazione del piano». Per allegato B «Regole tecniche e di sicurezza per l'accesso ai domini applicativi del C.N.S.D.».

Art. 2.

Adempimenti

1. I Comuni devono, entro il 31 ottobre 2005, provvedere a redigere il piano di sicurezza per la gestione delle postazioni di emissione secondo le regole tecniche fornite dal Ministero dell'Interno, in applicazione dell'art. 7-*vicies ter,* comma 2, della legge n. 43 del 31 marzo 2005.

Art. 3.

Allegati

1. L'allegato A «Piano di sicurezza comunale per la carta di identità elettronica: linee guida e metodologia per la redazione del piano» e l'allegato B «Regole tecniche e di sicurezza per l'accesso ai domini applicativi del C.N.S.D.» formano parte integrante e sostanziale del presente decreto.

Art. 4.

Funzioni dei comuni

1. I Comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato A, devono redigere il Piano di sicurezza comunale per la carta di identità elettronica.

2. I Comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato B, devono predisporre i necessari collegamenti all'Indice Nazionale delle Anagrafi (INA) presso il Centro Nazionale per i Servizi Demografici tramite porta di accesso ai domini applicativi del C.N.S.D., entro il 31 ottobre 2005.

Art. 5.

Redazione del piano di sicurezza comunale

1. I Comuni, ai fini della redazione del piano di sicurezza per la gestione delle postazioni di emissione della carta di identità elettronica, attuano la seguente procedura operativa:

a) nomina del responsabile comunale per la sicurezza degli accessi al C.N.S.D.;

b) redazione del Piano di sicurezza comunale per la C.I.E.;

c) il Piano di sicurezza comunale per la C.I.E. deve essere sottoposto all'approvazione della Prefettura-UTG.

Art. 6.

Collegamento al C.N.S.D.

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente, esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica della C.I.E. si connettono al Centro Nazionale per i Servizi Demografici tramite apposita porta di accesso, secondo le regole tecniche e di sicurezza di cui all'allegato B al presente decreto. Per l'attivazione del collegamento al C.N.S.D., le amministrazioni di cui al presente comma attuano la seguente procedura operativa:

a) attivazione e gestione delle «quantità di sicurezza, certificazione ed attivazione» fornite dal Ministero dell'Interno;

b) predisposizione ed attivazione della porta di accesso;

c) predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi del C.N.S.D.;

d) attivazione del collegamento all'INA tramite porta di accesso;

e) attivazione del collegamento tramite porta di accesso per l'emissione C.I.E.

Capo II

NORME PROCEDIMENTALI

Art. 7.

Nomina del responsabile comunale per la sicurezza degli accessi al C.N.S.D.

1. Il Sindaco è il Responsabile comunale per la sicurezza degli accessi al C.N.S.D. e può delegare formalmente tale incarico ad un funzionario comunale ritenuto idoneo ai sensi dell'art. 2 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223. L'atto di nomina è trasmesso al Ministero dell'Interno e alla Prefettura-UTG, secondo le modalità indicate sul sito, entro il 31 agosto 2005.

2. Per i comuni che hanno provveduto alla nomina del «responsabile del comune autorizzato all'attivazione del servizio di connessione al backbone applicativo Indice Nazionale Anagrafi» si intende che lo stesso assume anche il ruolo di responsabile comunale per la sicurezza degli accessi al C.N.S.D. a meno che non venga comunicato dal Sindaco un diverso nominativo entro il 31 agosto 2005.

3. All'atto della nomina il responsabile comunale per la sicurezza degli accessi al C.N.S.D. firma l'impegno alla riservatezza.

4. Il sindaco vigila sull'attività del delegato inviando semestralmente una relazione sull'operato del responsabile comunale per la sicurezza alla Prefettura-UTG.

5. Il Ministero dell'Interno provvede ad inviare al Sindaco le «quantità di sicurezza, certificazione ed attivazione» necessarie a:

a) abilitare la porta di accesso del Comune;

b) predisporre ed attivare i sistemi comunali per l'accesso ai servizi applicativi del C.N.S.D.;

c) attivare il collegamento all'INA tramite porta di accesso del Comune;

d) attivare il collegamento per l'emissione C.I.E. tramite porta di accesso del Comune.

6. Il Sindaco consegna al responsabile comunale per la sicurezza degli accessi al C.N.S.D. le «quantità di sicurezza, certificazione ed attivazione» per gli adempimenti di competenza.

7. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., ricevute le «quantità di sicurezza, certificazione ed attivazione», è responsabile della corretta attivazione della porta di accesso del Comune e di tutti i sistemi comunali che accedono ai servizi applicativi del C.N.S.D. (sistemi per i servizi INA, sistemi per emissione C.I.E., etc.).

Art. 8.

Redazione piano di sicurezza comunale

1. Il piano di sicurezza comunale deve essere redatto, in conformità alle regole tecniche e di sicurezza di cui all'allegato A, ed inviato, in formato digitale e cartaceo, ai fini della approvazione, alla Prefettura-UTG entro il 31 ottobre 2005. Successivamente il piano di sicurezza comunale deve essere aggiornato con cadenza semestrale.

Art. 9.

Approvazione piano di sicurezza comunale

1. Il piano di sicurezza comunale è emanato dal Sindaco che è responsabile della sua applicazione e della sua custodia in sicurezza presso la propria «segreteria atti riservati». Il piano di sicurezza viene trasmesso alla Prefettura-UTG, tramite CD-ROM, recante la firma indelebile del Sindaco e creato secondo le modalità previste dalla «quantità di sicurezza, attivazione e certificazione», in busta sigillata tramite ceralacca del Comune e consegnato per mezzo di messo comunale.

2. La Prefettura-UTG valuta, entro trenta giorni dalla consegna, il Piano di sicurezza comunale per la C.I.E. secondo i criteri forniti dal Ministero, con apposita verifica, ed esprime un parere, che può essere:

a) di approvazione totale;

b) di approvazione parziale: la Prefettura-UTG indica le modifiche da apportare al piano della sicurezza;

c) di non approvazione.

3. In caso di approvazione parziale, il Comune è tenuto a rivedere il piano di sicurezza in base alle osservazioni effettuate dalla Prefettura-UTG. Il piano di sicurezza con le modifiche effettuate deve essere quindi nuovamente sottoposto alla Prefettura-UTG, con allegata la lista di verifica delle modifiche effettuate, per l'approvazione.

4. In caso di mancata approvazione il Comune è tenuto a rivedere il piano di sicurezza in base alle osservazioni effettuate dalla Prefettura-UTG e completare le eventuali parti mancanti. Il piano di sicurezza con le modifiche effettuate deve essere quindi nuovamente sottoposto alla Prefettura-UTG per l'approvazione.

5. Qualora il piano di sicurezza comunale non venga redatto nei termini stabiliti dal presente decreto o non sia riveduto in caso di approvazione parziale, il prefetto, previa diffida, esercita i poteri sostitutivi previsti dalla normativa vigente.

6. La Prefettura-UTG custodisce i piani di sicurezza comunali e ne trasmette una copia al C.N.S.D., in formato digitale, tramite la porta di accesso della prefettura-UTG.

7. la Prefettura-UTG svolge funzioni di vigilanza sulla corretta applicazione del piano di sicurezza. A tal fine devono essere pianificate apposite visite ispettive.

8. Il Comune, ai fini dell'emissione C.I.E., deve rendere operativo il Piano di sicurezza comunale per la carta di identità elettronica approvato dalla Prefettura-UTG entro e non oltre il 31 dicembre 2005.

9. Il Comune aggiorna, ogni sei mesi, il piano di sicurezza comunale e invia le variazioni alla Prefettura-UTG unitamente alla lista di verifica delle modifiche effettuate per l'approvazione. La Prefettura-UTG trasmette gli aggiornamenti al C.N.S.D. tramite la porta di accesso della Prefettura-UTG.

10. Al fine di verificare la piena corrispondenza con le dotazioni autorizzate dal Ministero dell'Interno, prima della attivazione del piano di sicurezza il sindaco fa l'inventario delle «quantità di sicurezza, attivazione e certificazione», della porta di accesso comunale e delle postazioni C.I.E. con i relativi software, redigendo apposito verbale che, costituendo parte integrante del piano di sicurezza, verrà trasmesso unitamente allo stesso alla Prefettura-UTG.

11. Eventuali interventi modificativi o integrativi delle componenti software e hardware di cui al precedente comma, dovranno essere preventivamente autorizzati dal Ministero.

12. Le richieste di modifica o integrazione e le relative autorizzazioni devono essere conservate in originale secondo le modalità del successivo art. 10.

Art. 10.

Quantità di sicurezza, attivazione e certificazione

1. Le «quantità di sicurezza, attivazione e certificazione» sono fornite dal Ministero dell'Interno, protette da opportune credenziali, al Sindaco su supporto tecnologico-informatico di archiviazione che contiene i seguenti elementi:

a) credenziali digitali per l'identificazione univoca del Comune;

b) strumenti di sicurezza (agenti di controllo monitoraggio e allarme, certificati digitali, dotazioni di servizio) richiesti per l'attivazione della porta di accesso;

c) strumenti di sicurezza (certificati digitali, dotazioni di servizio) richiesti per l'attivazione delle postazioni comunali autorizzate all'accesso ai servizi applicativi del C.N.S.D. tramite porta di accesso;

d) strumenti di sicurezza (agenti di controllo monitoraggio e allarme, certificati digitali, dotazioni di servizio) richiesti per l'attivazione delle postazioni C.I.E.

2. Il Comune, prese in carico le «quantità di sicurezza, attivazione e certificazione», deve provvedere alla loro custodia in sicurezza, in coerenza con il Piano di sicurezza comunale per la C.I.E.

3. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., dopo apposita denuncia alle competenti autorità di polizia, deve immediatamente comunicare alla Prefettura-UTG ed al Ministero dell'Interno qualsiasi avvenimento che comprometta la sicurezza delle «quantità di sicurezza, attivazione e certificazione», quali smarrimento, furto o manomissione del relativo supporto tecnologico-informatico di archiviazione, tramite immediata comunicazione al call center del C.N.S.D.

Art. 11.

Attivazione della porta di accesso ai domini applicativi del C.N.S.D.

1. La porta di accesso del Comune ai domini applicativi del C.N.S.D. identifica il punto di accesso autorizzato, presente presso la struttura comunale, che consente la fruizione in sicurezza dei servizi erogati dal C.N.S.D. stesso. La porta di accesso certifica quindi il punto di origine delle comunicazioni, individuando univocamente il Comune che, tramite la porta di accesso, si collega al C.N.S.D. Nessuna altra modalità di comunicazione è quindi possibile tra Comune e C.N.S.D. Ciascun Comune deve dichiarare la porta di accesso che utilizza per le comunicazioni con il C.N.S.D., con modalità telematiche che saranno pubblicate sul sito del Ministero.

2. La procedura di attivazione di una porta di accesso deve essere effettuata dal responsabile comunale per la sicurezza degli accessi al C.N.S.D. utilizzando le credenziali e le «quantità di sicurezza, attivazione e certificazione» fornite dal Ministero dell'Interno. La procedura operativa si articola nelle seguenti fasi:

- messa a disposizione delle componenti hardware conformi alle regole tecniche e di sicurezza indicate dal Ministero, riportate nell'allegato B al presente decreto, e pubblicate nel sito;

- configurazione dell'infrastruttura di rete comunale secondo le regole tecniche e di sicurezza indicate dal Ministero, riportate nell'allegato B al presente decreto, e pubblicate nel sito;

- attivazione, a cura del responsabile della sicurezza, e nel rispetto delle regole di sicurezza del C.N.S.D., della porta di accesso. L'attivazione consta delle seguenti fasi:

a) abilitazione della porta di accesso tramite «quantità di sicurezza, attivazione e certificazione», attivazione del canale Backbone del C.N.S.D., attivazione degli agenti di controllo monitoraggio e allarme,

predisposizione del certificato digitale server per il colloquio secondo standard SSL (Secure Socket Layer) con i sistemi comunali;

b) registrazione, presso il C.N.S.D., della porta di accesso tramite «quantità di sicurezza, attivazione e certificazione»;

c) verifica, sulla base della lista fornita con le «quantità di sicurezza, attivazione e certificazione», che sulla porta di accesso sia presente tutto il software autorizzato e necessario e che non sia presente software non necessario e non autorizzato. A seguito della verifica viene compilato il verbale di cui al comma 10 dell'art. 9. A garanzia del funzionamento in sicurezza della porta, il software autorizzato viene firmato tramite certificati digitali forniti con le «quantità di sicurezza, attivazione e certificazione» al fine di impedirne qualsiasi manomissione. Una porta su cui sia presente software non autorizzato non viene considerata abilitata alle sue funzioni e quindi qualsiasi operazione effettuata tramite la stessa è da considerare a tutti gli effetti una violazione della sicurezza;

d) prova di comunicazione, effettuata tramite dotazione di servizio fornita, della porta di accesso in termini di sicurezza e di dimensionamento dei flussi di comunicazione con il C.N.S.D.

3. Alla conclusione delle suddette fasi il Ministero dell'Interno - C.N.S.D. certifica la porta di accesso in funzione dei risultati della prova di cui al punto precedente. Farà seguito una comunicazione di certificazione che perverrà al Comune sulla medesima porta di accesso.

4. Alla corretta conclusione delle fasi sopra descritte, la porta di accesso si ritiene attivata e, quindi, è ritenuta un punto di accesso al C.N.S.D. riconosciuto ed autorizzato. La porta di accesso rappresenta il punto di presa in carico delle comunicazioni provenienti dal Comune relative ai flussi di aggiornamento INA e di emissione della C.I.E. e trasmissione al C.N.S.D., tramite Backbone, di tali comunicazioni in apposita «busta di e-gov» creata dalla porta stessa secondo le specifiche del Sistema Pubblico di Connettività.

5. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D. deve controllare la corretta attivazione della porta di accesso, secondo le regole tecniche e di sicurezza riportate nel presente decreto.

6. Presso ogni Comune, entro il 30 settembre 2005, deve essere attivata una porta di accesso del Comune. Per i piccoli comuni, se l'unica postazione presente è la postazione attualmente usata per l'invio dei dati AIRE su Backbone AIRE, la stessa deve essere utilizzata, previa attivazione secondo la procedura descritta nel presente articolo, come porta di accesso del Comune mantenendo anche le attuali funzioni svolte per l'AIRE.

7. La porta di accesso della Prefettura-UTG ai domini applicativi del C.N.S.D. identifica il punto di accesso autorizzato, presente presso la Prefettura-UTG, che consente l'accesso, in sicurezza, ai servizi erogati dal C.N.S.D. stesso. Presso ogni Prefettura-UTG, entro il 31 ottobre 2005, deve essere attivata una porta di accesso della Prefettura-UTG.

Art. 12.

Abilitazione dei sistemi anagrafici comunali ai servizi applicativi del C.N.S.D.

1. I sistemi comunali devono accedere ai servizi del C.N.S.D. esclusivamente tramite la porta di accesso. La procedura per l'attivazione di un sistema anagrafico comunale è la seguente:

a) abilitazione e registrazione del sistema comunale alla porta di accesso per lo specifico servizio applicativo del C.N.S.D. tramite «quantità di sicurezza, attivazione e certificazione»: dal supporto tecnologico-informatico, di cui all'art. 8, fornito dal Ministero dell'Interno vengono scaricati sul sistema comunale i certificati digitali client forniti per l'abilitazione alla comunicazione, secondo standard SSL, del sistema comunale stesso con la porta di accesso;

b) prova di comunicazione, effettuata tramite dotazione di servizio fornita, relativa alla corretta configurazione e funzionamento dei canali di comunicazione.

Le relative regole tecniche e di sicurezza di dettaglio sono riportate nell'allegato B al presente decreto.

2. Al termine delle fasi sopra descritte, il sistema comunale si ritiene attivato e, quindi, è autorizzato ad inviare le informazioni (secondo protocollo XML SOAP o Post HTTP XML) alla porta di accesso che crea la busta di e-gov e la trasmette automaticamente, tramite Backbone, al servizio applicativo del C.N.S.D. per cui è stata effettuata l'attivazione.

3. I formati XML per la comunicazione tra sistema comunale e porta di accesso sono forniti dal Ministero dell'Interno.

4. I sistemi comunali che accedono ai servizi del C.N.S.D. devono essere registrati presso la porta di accesso.

5. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D. ha il compito di controllare l'attivazione e la registrazione dei sistemi comunali, secondo le reali esigenze.

6. I livelli di sicurezza relativi ai sistemi e ai prodotti della porta di accesso sono certificati, sulla base degli standard internazionali, dal Ministero dell'Interno.

Art. 13.

Attivazione del collegamento all'INA

1. I sistemi comunali utilizzati per l'accesso all'INA, devono essere attivati per l'accesso al servizio INA del C.N.S.D., tramite porta di accesso, entro e non oltre il 31 ottobre 2005, coerentemente con il disposto dell'art. 7-*vicies ter* della legge n. 43 del 31 marzo 2005.

2. I formati XML che devono essere utilizzati per inviare le interrogazioni INA e gli aggiornamenti INA, sono forniti e pubblicati dal Ministero dell'Interno sul sito.

Art. 14

Emissione CIE

1. Le postazioni C.I.E. devono accedere ai servizi del C.N.S.D. e, attraverso questo, a SSCE esclusivamente tramite porta di accesso. Le postazioni C.I.E. possono essere:

a) postazioni C.I.E. di «Front office» deputate all'acquisizione dei dati anagrafici dei richiedenti e alla consegna e attivazione della C.I.E.;

b) postazioni C.I.E. di Back Office per l'allestimento della C.I.E. deputate alla predisposizione e stampa dei supporti C.I.E. sulla base dei dati anagrafici acquisiti al Front office;

c) postazioni C.I.E. di Back Office per l'elaborazione e le comunicazioni di informazioni con il C.N.S.D. e, attraverso questo, con il SSCE;

d) postazioni C.I.E. che integrino due o più delle tipologie precedenti.

2. Per qualsiasi tipologia di postazione C.I.E. deve essere seguita la seguente procedura di attivazione:

a) abilitazione della postazione C.I.E. tramite «quantità di sicurezza, attivazione e certificazione»;

b) registrazione, da effettuarsi prima della installazione del software di emissione C.I.E., della postazione C.I.E. sulla porta di accesso tramite «quantità di sicurezza, attivazione e certificazione»; a seguito di tale registrazione viene assegnato automaticamente un identificativo univoco alla postazione di emissione che la abilita all'emissione della C.I.E. e che viene utilizzato per tutte le comunicazioni con il Ministero dell'Interno ed il circuito di emissione della C.I.E.;

c) attivazione degli agenti di controllo, monitoraggio e allarme forniti dal Ministero dell'Interno e del software di emissione C.I.E.;

d) installazione e attivazione del software di emissione C.I.E.;

e) verifica, sulla base della lista fornita con le «quantità di sicurezza, attivazione e certificazione», che sulla postazione C.I.E. sia presente tutto il software autorizzato e necessario e che non sia presente software non necessario e non autorizzato. A seguito della verifica viene compilato il verbale di cui al comma 10 dell'art. 9. A garanzia del funzionamento in sicurezza della postazione C.I.E., il software autorizzato viene firmato tramite certificati digitali forniti con le «quantità di sicurezza, attivazione e certificazione» al fine di impedirne qualsiasi manomissione. Una postazione C.I.E. su cui sia presente software non autorizzato non viene considerata abilitata alle sue funzioni e quindi qualsiasi operazione effettuata tramite la stessa è da considerare a tutti gli effetti una violazione della sicurezza;

f) prova, effettuata tramite dotazione di servizio fornita, della corretta configurazione dei canali di comunicazione.

Le relative regole tecniche e di sicurezza di dettaglio sono riportate nell'allegato B al presente decreto.

3. Al termine delle fasi sopra descritte, la postazione C.I.E. si ritiene attivata e, quindi, è autorizzata ad inviare i flussi relativi all'emissione C.I.E. alla porta di accesso. Tramite porta di accesso sono garantiti i servizi di sicurezza per l'accesso ai sistemi distribuiti di verifica dello stato dei certificati C.I.E.

4. Le regole tecniche e di sicurezza di cui agli allegati A e B al presente decreto devono essere rispettate anche dagli eventuali centri di allestimento periferici che potrebbero essere costituiti per la stampa della C.I.E.

I Sindaci dei Comuni presso i quali saranno costituiti i centri di allestimento dovranno nominare il responsabile del centro di allestimento per la sicurezza degli accessi al C.N.S.D.

5. Il Ministero dell'Interno controlla e verifica il rispetto dei vincoli di sicurezza relativi all'intero processo di emissione C.I.E. avvalendosi anche delle proprie infrastrutture tecnologiche di controllo, monitoraggio e allarme.

6. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., ha il compito di controllare l'attivazione e la registrazione delle postazioni C.I.E.

7. I livelli di sicurezza relativi ai sistemi e ai prodotti del circuito di emissione della C.I.E. sono certificati, sulla base degli standard internazionali, dal Ministero dell'Interno.

Roma, 2 agosto 2005

Il Ministro: PISANU

ALLEGATO A

LINEE GUIDA E METODOLOGIA PER LA REDAZIONE DEL PIANO

INDICE

Allegato 1 — RIFERIMENTI NORMATIVI E REGOLAMENTARI

Allegato 2 — POLITICHE DI SICUREZZA E METODOLOGIA DI ATTUAZIONE DEL PIANO DELLA SICUREZZA

Allegato 3 — REDAZIONE DEL PIANO DI SICUREZZA VERSIONE ALFA: DEFINIZIONE STRUTTURA DI RIFERIMENTO, ANALISI E CLASSIFICAZIONE DELLE PROCEDURE OPERATIVE

Allegato 4 — SCHEDE DI ATTUAZIONE DELLA VERSIONE ALFA DEL PIANO SICUREZZA DEI COMUNI: CLASSIFICAZIONE MINACCE, VULNERABILITÀ E VALUTAZIONE DEL RISCHIO

ALLEGATO 5 — MONITORAGGIO E VALIDAZIONE DEL PIANO

ALLEGATO 6 — MANUTENZIONE ED EVOLUZIONE DEL PIANO

ALLEGATO 7 — DOCUMENTO OPERATIVO PER I COMUNI
AI FINI DELLA COMPILAZIONE DEL PIANO DI SICUREZZA

1. Scopo e campo di applicazione

Questo documento descrive la metodologia e fornisce gli strumenti e le indicazioni necessari alla revisione, all'attuazione, alla gestione ed alla manutenzione del Piano di Sicurezza Comunale nell'ambito dei processi relativi alle attività di rilascio ed uso della Carta d'Identità Elettronica. Il documento è stato realizzato con l'obiettivo di consentire al Comune di redigere o aggiornare il proprio piano di sicurezza e di curarne l'attuazione.

La scelta di suddividere questo documento in capitoli ed allegati, deriva dalla necessità di fornire uno strumento snello e di semplice impiego, di supporto alla redazione ed all'attuazione del piano di sicurezza.

I capitoli successivi, strutturati in allegati, sono di seguito brevemente descritti:

Allegato 1. Riferimenti normativi e regolamentari.

Allegato 2. Metodologia di attuazione del piano di sicurezza.

Allegato 3. Piano di sicurezza versione alfa che il Comune deve utilizzare e specializzare per la realizzazione del suo primo piano di sicurezza.

Allegato 4. Schede di attuazione del piano di sicurezza versione alfa: fornisce gli strumenti che consentono al Comune di attuare il piano di sicurezza.

Allegato 5. Monitoraggio e validazione: fornisce gli strumenti che consentono al Comune di monitorare e validare l'attuazione del piano di sicurezza.

Allegato 6. Manutenzione ed evoluzione del piano: fornisce la base per l'elaborazione del piano di sicurezza aggiornato (versione beta) sulla base dei risultati delle attività di monitoraggio previste nel piano versione alfa.

Allegato 7. Indice del Piano di Sicurezza: costituisce il documento operativo per i Comuni ai fini della compilazione del Piano di Sicurezza.

2. Riferimenti

[1] BS7799-2:2002
[2] ISO/IEC 17799:2000
[3] ISO 9001:2000
[4] Linee Guida OCSE/OECD
[5] ISO/IEC TR 13335 (parti 1, 2, 3, 4, 5)
[6] IT SEC (Applicato in Europa)
[7] ISO/IEC 15408 (Common Criteria – evoluzione ed integrazione dei due precedenti)
[8] Raccomandazione del Consiglio dell'Unione Europea - 95/144/CE- 7 aprile 1995: applicazione dei criteri per la valutazione della sicurezza della tecnologia dell'informazione
[9] Legge 675/96
[10] DPR 513/97: regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59,
[11] DPCM 22 ottobre 1999 n. 437: regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, N. 191.
[12] DPR 318/99
[13] Risoluzione del Consiglio dell'Unione Europea del 6 dicembre 2001: approccio comune nel settore della sicurezza delle reti e dell'informazione.
[14] Dlgs. 28 dicembre 2001, n, 467, che indica le "Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della legge 24 marzo 2001, n. 127"
[15] Direttiva (denominata direttiva Stanca) 16 gennaio 2002 del Dipartimento per l'innovazione e le tecnologie, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;
[16] Decreto del Ministro dell'Interno in data 23 aprile 2002, costituzione , presso la Direzione Centrale per i Servizi Demografici il Centro Nazionale Servizi Demografici
[17] Direttiva del Ministro Stanca 9 dicembre 2002 "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali".
[18] Dlgs 196/2003
[19] Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni: "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione", marzo 2004.
[20] Legge 43/2005
[21] Decreto legge 31 marzo 2005 n. 44 convertito nella legge 31 maggio 2005 n. 88
[22] Regole tecniche e di sicurezza per l'accesso ai domini applicativi del CNSD

3. Definizioni e acronimi

CIE	Carta d'Identità Elettronica
Informazione	Dato o dati conservati o processati nei sistemi o su dispositivi rimovibili durante l'esecuzione di processi organizzativi
Sicurezza	Protezione dell'informazione dalla distruzione, dalle modifiche e dalla divulgazione non autorizzate.
Riservatezza	Protezione contro la divulgazione di informazioni senza il consenso del proprietario
Integrità	Protezione contro la modifica, la creazione o la replica non autorizzata delle informazioni.
Disponibilità	Protezione contro ritardi non accettabili nell'accesso autorizzato alle informazioni.
Autenticità	Principio che assicura che un'informazione sia stata fornita da chi sostiene essere l'autore e non è stata alterata in nessun modo da una terza parte.
Responsabilità	Principio che garantisce l'imputabilità ad ogni soggetto degli effetti di ciascuna azione dal medesimo compiuta.
Asset	Qualunque tipo di risorsa utile alla realizzazione di un processo.
Affidabilità	Principio che indica la capacità di un asset di sopportare senza danni irreparabili, l'impatto di eventi imprevisti.
CNSD	Il Centro Nazionale dei Servizi Demografici del Ministero dell'Interno costituito con il Decreto del Ministro dell'Interno del 23 aprile 2002
SSCE	Il sistema di sicurezza del circuito di emissione dei documenti di identità elettronica
INA	L'Indice nazionale delle anagrafi istituito con legge 28 febbraio 2001, n. 26, sostituita dalla legge 31.5.2005, n. 88, per la fornitura dei servizi di convalida anagrafica durante l'emissione e l'uso del documento
Backbone CNSD	La dorsale di sicurezza e certificazione del CNSD per l'accesso ai servizi applicativi del CNSD
Postazione di Emissione	Postazione dedicata ai processi di emissione CIE sia di front office che di back office
MEF	Ministero Economia e Finanze
MI	Ministero dell'Interno
SPC	Il Sistema Pubblico di Connettività di cui al Decreto legislativo n. 42 del 28 febbraio 2005.
Porta di accesso ai domini	La porta di accesso, attraverso il Backbone del CNSD, ai servizi del CNSD, secondo standard "busta di e-gov" di SPC.

applicativi del CNSD	
Busta di e-gov	Il formato comune di interscambio tra porte di dominio di enti diversi.
Protocollo XML-Soap	Il protocollo di trasporto della "busta di e-gov del CNSD" che uniforma i messaggi scambiati con la Porta di accesso.
Protocollo post http XML	Il protocollo di trasmissione di un evento in formato XML alla Porta di accesso.
Quantità di sicurezza, attivazione e certificazione	Le credenziali digitali ed i software di sicurezza, monitoraggio ed allarmi forniti dal Ministero dell'Interno per la registrazione e l'attivazione delle porte di accesso.
Quantità di sicurezza	Supporto tecnologico-informatico di archiviazione fornito dal Ministero e contenente le credenziali richieste per la comunicazione con i servizi di emissione CIE.
Modello asincrono di emissione CIE	Il modello asincrono di emissione CIE consente ai Comuni di "separare" il processo di emissione in più fasi atomiche, ognuna indipendente dalle altre.
Sistema degli agenti di monitoraggio ed allarmi	Sistema di controllo e certificazione dello stato di funzionamento ed operatività sia delle postazioni di front office e di back office, sia dei punti di accesso ai domini applicativi del CNSD.
Responsabile della sicurezza	Responsabile comunale che definisce, aggiorna, approva e controlla le regole di sicurezza del Comune inerenti l'intera infrastruttura di emissione ed uso della CIE.

4. Introduzione

Con decreto del Ministro dell'Interno in data 23 aprile 2002 è stato costituito, presso la Direzione Centrale per i Servizi Demografici, il Centro Nazionale Servizi Demografici (CNSD). Il Centro Nazionale nasce come conseguenza logico-normativa degli interventi legislativi svolti negli ultimi anni in materia di AIRE, di CIE, di INA e, non ultimo, di Stato Civile. Al CNSD è affidata, tra gli altri incarichi, la gestione unitaria delle attività e delle infrastrutture informatiche centrali relative al rilascio della Carta d'identità elettronica e alla sua utilizzazione per l'accesso ai servizi erogati dalle Amministrazioni Pubbliche centrali e locali.
L'obiettivo è di gestire unitariamente le attività di tutte le attuali infrastrutture informatiche centrali di interesse dei Servizi demografici, e di quelle in via di realizzazione, al fine di garantire la trasparenza e la sicurezza dei processi di autenticazione e di convalida dei dati anagrafici.

Il Centro Nazionale Servizi Demografici e, a livello locale, i Comuni, si avvalgono delle seguenti infrastrutture di sicurezza:

• Backbone di Sicurezza del CNSD e Porta di accesso ai domini applicativi del CNSD presente presso l'infrastruttura Comunale.

• Sistema di Sicurezza del Circuito di Emissione delle carte d'identità e dei documenti d'identità elettronici.

In particolare, la porta di accesso ai domini applicativi del CNSD rappresenta il punto di presa in carico delle comunicazioni provenienti dal Comune (aggiornamento INA, flussi di emissione della CIE, altri servizi anagrafici) e del loro successivo inoltro al CNSD. Tale porta di accesso certifica il punto di origine delle comunicazioni, individuando univocamente il Comune che comunica con il CNSD: **tutte le comunicazioni devono quindi avvenire esclusivamente tramite la porta di accesso del Comune ai domini applicativi del CNSD**.

5. Obiettivi

L'attuazione del piano di sicurezza presso i Comuni coinvolge gli aspetti organizzativi, tecnologici e logistici. Al fine di garantire tale attuazione è necessario procedere alla stesura di un primo piano organico di sicurezza che deve essere specializzato dai Comuni, ovvero reso coerente al concreto modello tecnico-organizzativo esistente presso il Comune, sia nella fase di prima attuazione, sia in quella di gestione a regime dello stesso.

L'obiettivo primario di questo documento è quindi quello di fornire ai Comuni uno strumento metodologico ed un insieme di linee guida che consentano di realizzare, adeguare e gestire i piani di sicurezza CIE in modo tale da garantire:

- la riservatezza delle informazioni,
- l'integrità delle informazioni,
- la disponibilità delle informazioni,
- la continuità delle attività legate ai processi,
- la realizzazione di un sistema flessibile idoneo a recepire, nel tempo, eventuali aggiornamenti e modifiche.

6. Principi generali

Il presente piano della sicurezza comunale CIE si basa sui i seguenti principi generali:

a) Tutti gli accessi ai servizi applicativi del CNSD devono avvenire tramite la porta di accesso del Comune ai domini applicativi del CNSD;
b) Tutte le informazioni (dati, documenti, archivi, …) devono essere protette e mantenute;
c) Per la riservatezza dei contenuti scambiati, la sicurezza deve essere garantita anche a livello delle reti di comunicazioni dati;
d) Deve essere gestita la sicurezza sia di tutti gli apparati inerenti la struttura comunale di emissione ed uso della CIE, sia del materiale di consumo considerato sensibile ai fini della sicurezza;

e) Tutte le registrazioni devono essere oggetto di monitoraggio costante (manuale o automatico);
f) Devono essere predisposte adeguate misure di sicurezza per l'accesso ai locali che ospitano le postazioni di front office, back office e la Porta di accesso al CNSD, nonché tutto il materiale impiegato nei processi di rilascio della CIE;
g) Ogni eventuale incidente o evento straordinario che possa pregiudicare la sicurezza deve essere oggetto di analisi e di rapporto scritto;
h) La Porta di accesso ai domini applicativi del CNSD e le postazioni di emissione CIE, sia di back office che di front office, devono essere utilizzati ai soli fini del rilascio ed uso della CIE e per l'accesso ai servizi del CNSD;
i) Tutti i progetti di nuove applicazioni/servizi devono essere inseriti nel piano per la sicurezza;
j) Tutte le modifiche, eventualmente apportate ai processi organizzativi interni al Comune, devono essere inserite nel Piano per la Sicurezza che va nuovamente trasmesso alla Prefettura per l'approvazione.
k) Per tutti i processi o macroprocessi CIE, deve essere individuato un responsabile di riferimento.

6.1. Responsabilità

Il Responsabile della Sicurezza CIE risponde dell'attuazione del piano della sicurezza ed è pertanto tenuto a far applicare i procedimenti di sicurezza individuando le specifiche unità di personale impiegate nei macroprocessi CIE.

6.2. Revisione ed adeguamento del piano

Il piano della sicurezza deve essere sottoposto a verifiche periodiche, in ogni caso almeno una volta l'anno. Il piano deve essere aggiornato con una nuova analisi dei rischi ogniqualvolta si verifichino circostanze che possano comprometterne la validità e l'efficacia.

6.3. Vincoli

Nel documento sono evidenziate le procedure di sicurezza vincolanti, che devono obbligatoriamente essere inserite nel piano di sicurezza in quanto relative a minacce alla sicurezza il cui trattamento è ritenuto prioritario.

7. Uso degli allegati e risultati attesi

Di seguito, si riporta l'elenco degli allegati ed una breve descrizione dei contenuti.

Allegato 1. Riferimento normativo e regolamentare;

Allegato 2. Metodologia di realizzazione del piano della sicurezza secondo un insieme di fasi predeterminate;

Allegato 3. Piano di sicurezza versione alfa che il Comune deve utilizzare e specializzare per la realizzazione del suo primo piano di sicurezza;

Allegato 4. Schede di attuazione del piano alfa, che consentono al Comune di rendere operativo il piano di sicurezza;

Allegato 5. Schede di monitoraggio che consentono al Comune di monitorare e validare l'attuazione del piano di sicurezza;
Allegato 6. Schede per l'elaborazione del piano della sicurezza versione beta, redatto sulla base dei risultati dell'attività di monitoraggio.
Allegato 7. Indice del piano di sicurezza, che costuisce uno strumento di supporto ai Comuni per la compilazione del suddetto piano.

La metodologia adottata per la realizzazione la gestione del piano della sicurezza, prevede quattro fasi:
a) Individuazione e classificazione dei rischi e definizione degli interventi per mitigare/evitare i rischi classificati come critici.
b) Attuazione degli interventi.
c) Monitoraggio e validazione degli interventi.
d) Revisione del piano, esame delle debolezze, riesame delle criticità.

Gli allegati 3, 4, 5 e 6 consentono al Comune di gestire ed attuare le quattro fasi qui accennate.

8. La metodologia utilizzata per l'attuazione del piano della sicurezza

La metodologia utilizzata per il raggiungimento degli obiettivi è la metodologia PDCA (Plan, Do, Check, Act).
Con questo acronimo si definisce la metodologia che partendo da un'idea di fondo, la sviluppa in modo circolare per verificarne i presupposti stessi.
L'acronimo PDCA individua 4 fasi principali:

PLAN La fase di Plan consiste nell'identificazione del problema, nella sua analisi, nell'individuazione delle cause reali nonchè nella definizione e pianificazione delle azioni correttive.

DO La fase di Do consiste nella preparazione ed applicazione delle azioni pianificate.

CHECK La fase di Check consiste nella verifica dei i risultati raggiunti a fronte degli obiettivi attesi.

ACT La fase di Act consiste nel consolidamento dei risultati raggiunti, oppure nell'attivazione di un nuovo ciclo PDCA, con l'introduzione di opportuni correttivi, se non sono stati raggiunti i risultati attesi.

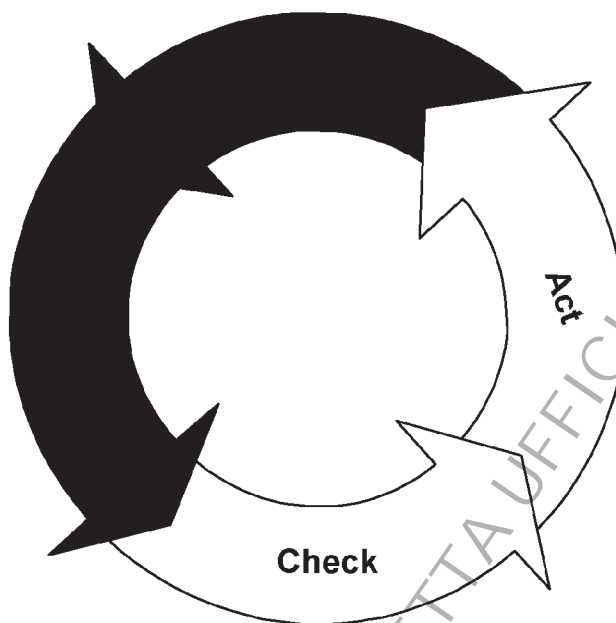



Figura 1 – Schema PDCA

La declinazione del modello metodologico PDCA, nell'ambito relativo alla sicurezza, vede contemplati i seguenti passi principali:

PLAN Definizione del piano della Sicurezza.
DO Implementazione e attuazione.
CHECK Monitoraggio e validazione.
ACT Manutenzione ed evoluzione.

Allegato 1
RIFERIMENTI NORMATIVI E REGOLAMENTARI

1. Descrizione delle norme relative alla "sicurezza"

1.1. Ambiti relativi alla sicurezza

Gli ambiti normativi relativi alla sicurezza, sono classificati nel modo seguente:

- Norme funzionali relative ai prodotti, aventi come scopo principale la ricerca dell'interoperabilità dei sistemi informatici;
- Criteri di valutazione della fiducia riposta nella sicurezza (assurance) di specifici sistemi e prodotti informatici;
    - TCSEC (Applicato in ambito USA);
    - ITSEC (Applicato in Europa);
    - ISO /IEC 15408;
    - Direttiva "Stanca" sulla sicurezza ITC;
- Norme relative al sistema di gestione della sicurezza;
    - ISO/IEC TR 13335 (parti 1,2,3,4);
    - BS7799 (parti 1 e 2);
    - ISO/IEC 17799:2000 (recepisce la parte 1 delle BS7799);
- Vigenti normative nazionali ed europee.

1.2. La sicurezza nell'ITC (Tecnologie dell'Informazione e della Comunicazione)

Con il termine "sicurezza" s'intende l'insieme di misure, di carattere organizzativo e tecnologico, tese ad assicurare a ciascun utente autorizzato (e a nessun altro) esclusivamente i servizi previsti per l'utente stesso, nei tempi e nelle modalità stabilite. Più formalmente, secondo la nota definizione ISO, la sicurezza è "l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite" e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco.

Gli incidenti di sicurezza possono essere causati da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi,
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.),
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.),
- persone interne all'organizzazione.

e possono essere identificati come:

- accidentali,
- deliberati.

Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma significa, in particolare, collocare ciascuna delle contromisure individuate in una politica organica di sicurezza che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed

organizzativa in cui il sistema di servizi opera e che giustifichi ciascuna contromisura in un quadro complessivo.

1.3. Il contesto internazionale

A livello internazionale il tema sicurezza è affrontato in modo sistematico dal 1995 (norme BS7799). Le norme introducono nel settore della sicurezza il concetto di "Sistema di Gestione" che permette di tenere sotto controllo nel tempo i processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, di procedure formali e di canali di comunicazione.
Principale obiettivo di un sistema di sicurezza è la salvaguardia delle informazioni. A tal proposito è fondamentale individuare quali informazioni proteggere e quale livello di protezione assegnare a ciascuna di esse.
Lo standard BS7799 individua tre aspetti fondamentali relativi alla sicurezza delle informazioni:

- **Confidenzialità** solo gli utenti autorizzati possono accedere alle informazioni necessarie.
- **Integrità** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati.
- **Disponibilità** le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Fra le risorse (asset) da tutelare rientrano certamente:
- dati digitali,
- documenti cartacei,
- flussi informativi,

nonché componenti materiali come:
- computer,
- reti,

ma anche:
- il personale,

e non ultimo:
- gli edifici,
- gli uffici.

L'approccio alla sicurezza deve avvenire in una logica di prevenzione (risk management) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.
L'architettura per rispondere alle esigenze di sicurezza è costituita da 3 elementi fondamentali:
- le politiche dell'organizzazione,
- gli strumenti organizzativi e tecnologici,
- gli atteggiamenti individuali.

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

- mantenersi aggiornata su nuove minacce e vulnerabilità, e prenderle in considerazione in modo sistematico,
- trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo dal sistema,
- sapere quando politiche di sicurezza e procedure non sono implementate, in tempo utile per prevenire danni,
- implementare politiche e procedure di primaria importanza.

Le BS7799 affrontano il problema sicurezza ad alto livello, indipendentemente dalla tecnologia, concentrandosi principalmente sulla gestione della sicurezza.

1.3.1. Applicare le BS7799

Per la corretta applicazione delle norme BS7799 è necessario predisporre ed attuare adeguati strumenti e controlli per la gestione e il controllo della sicurezza.
Tali norme forniscono un'utile base per l'effettiva gestione della sicurezza, grazie anche alla presenza di indicazioni relative alla creazione di politiche di sicurezza, alla formazione e sensibilizzazione di tutto il personale, nonché alle azioni da intraprendere per garantire la continuità delle attività.
L'applicazione delle BS7799 consente di:

- verificare l'adeguatezza dei processi per il trattamento delle informazioni,
- dimostrare che sono rispettati i requisiti espressi in contratti, leggi o regolamenti,
- valutare il rapporto costi/benefici dei propri investimenti.

La costruzione di un sistema di sicurezza valido, adeguato ed efficace, ha per il Comune una ricaduta positiva in termini di immagine verso l'esterno.

La metodologia BS7799 si articola nelle seguenti fasi principali:

- analisi conoscitiva dell'organizzazione,
- politiche generali di sicurezza delle informazioni,
- analisi e gestione del rischio.

1.3.2. Composizione delle norme BS7799

Le norme sono divise in due parti:

- BS7799:1 ovvero ISO/IEC 17799:2000
    - Riporta e descrive 127 linee guida sulla sicurezza delle informazioni. Strutturato in 10 capitoli, è di supporto alla redazione ed all'attuazione del piano di sicurezza.
- BS7799-2
    - Riporta indicazioni e fornisce dettagli sull'applicazione delle BS7799:1.

I dieci capitoli in cui sono raccolte le 127 linee guida per la sicurezza sono:

- Politica di sicurezza.

- Organizzazione per la sicurezza.
- Controllo e classificazione delle risorse.
- Sicurezza del personale.
- Sicurezza materiale e ambientale.
- Gestione operativa e comunicazione.
- Controllo degli accessi.
- Sviluppo e manutenzione dei sistemi.
- Gestione della continuità delle attività.
- Conformità.

In tale insieme vanno selezionate, attraverso il processo di analisi del rischio illustrato nei capitoli successivi, quelle linee guida che soddisfano le esigenze di sicurezza del Comune. Le linee guida prescelte vanno così a costituire un insieme di controlli di sicurezza che il Comune si impegna ad attuare.

Tali controlli devono essere realizzati attraverso:
- meccanismi hardware o software (sistemi di autenticazione tramite password, token card, smart card, prodotti per la protezione crittografica dei dati, firewall, etc.);
- sistemi anti intrusione, telecamere, tornelli, casseforti, contenitori ignifughi, etc.;
- la creazione di apposite strutture o funzioni all'interno dell'organizzazione e la definizione di procedure organizzative (ad esempio l'istituzione di un forum per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di formazione periodica del personale, le procedure per l'accettazione di ospiti all'interno dell'organizzazione, ecc.).

Le norme BS7799-2 forniscono indicazioni e spiegazioni su come applicare le norme BS7799:1 (ISO/IEC 17799:2000).
Le BS 7799-2 forniscono una base eccellente su cui costruire i controlli di gestione necessari per raggiungere gli obiettivi di sicurezza prefissati, gestire il rischio, assicurare un controllo efficace e definire miglioramenti, ove necessario.

1.4. Il contesto nazionale

A livello nazionale, nel corso degli anni, numerose sono state le iniziative legislative che hanno interessato il problema della sicurezza informatica. Tra queste si richiama la cosiddetta direttiva "Stanca" sulla Sicurezza nelle tecnologie dell'informazione e della comunicazione.
Tale direttiva fornisce (allegati 1 e 2 alla direttiva) indicazioni di carattere istituzionale (costituzione del comitato nazionale per la sicurezza ITC), un questionario di autovalutazione sulla sicurezza ed un insieme di indicazioni di massima (base minima di sicurezza) per la redazione e gestione del piano di sicurezza di una pubblica amministrazione.
Un'ulteriore, importante contributo in materia, si è avuto, nel mese di marzo 2004, con il documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" redatto dal "Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni".
Tale documento contiene le proposte preliminari concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, così come

richiesto dall'articolo 2, comma 1 del decreto istitutivo del Comitato stesso. Inoltre esso prevede che una metodologia di analisi del rischio:

a) sia progettata in conformità alle norme BS7799, già selezionate per la redazione di questo documento e che ne costituiscono, quindi, il naturale riferimento per attuazione del piano di sicurezza presso i comuni.
b) preveda almeno 4 fasi consequenziali e interrelate:
    a. pianificazione dell'intervento;
    b. valutazione del Rischio;
    c. gestione del Rischio;
    d. report alla Direzione.

    Queste fasi risultano perfettamente sovrapponibili alle quattro fasi della metodologia PDCA precedentemente descritta, selezionata per l'attuazione del piano della sicurezza dei Comuni.

1.5. Prospetto sintetico delle norme e degli standard di riferimento

[1] BS7799-2:2002
[2] ISO/IEC 17799:2000
[3] ISO 9001:2000
[4] Linee Guida OCSE/OECD
[5] ISO/IEC TR 13335 (parti 1, 2, 3, 4, 5)
[6] IT SEC (Applicato in Europa)
[7] ISO/IEC 15408 (Common Criteria – evoluzione ed integrazione dei due precedenti)
[8] Raccomandazione del Consiglio dell'Unione Europea - 95/144/CE- 7 aprile 1995: applicazione dei criteri per la valutazione della sicurezza della tecnologia dell'informazione
[9] Legge 675/96
[10] DPR 513/97: regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59,
[11] DPCM 22 ottobre 1999 n. 437: regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, N. 191.
[12] DPR 318/99
[13] Risoluzione del Consiglio dell'Unione Europea del 6 dicembre 2001: approccio comune nel settore della sicurezza delle reti e dell'informazione.
[14] Dlgs. 28 dicembre 2001, n, 467, che indica le "Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della legge 24 marzo 2001, n. 127"
[15] Direttiva (denominata direttiva Stanca) 16 gennaio 2002 del Dipartimento per l'innovazione e le tecnologie, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;
[16] Decreto del Ministro dell'Interno in data 23 aprile 2002, costituzione , presso la Direzione Centrale per i Servizi Demografici il Centro Nazionale Servizi Demografici

[17] Direttiva del Ministro Stanca 9 dicembre 2002 "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali".
[18] Dlgs 196/2003
[19] Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni: "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione", marzo 2004.
[20] Legge 43/2005
[21] Decreto legge 31 marzo 2005 n. 44 convertito nella legge 31 maggio 2005 n. 88
[22] Regole tecniche e di sicurezza per l'accesso ai domini applicativi del CNSD

Allegato 2
POLITICHE DI SICUREZZA E METODOLOGIA DI ATTUAZIONE DEL PIANO DELLA SICUREZZA

1.Ambito di applicazione del Piano della Sicurezza Comunale

L'ambito di applicazione fa riferimento alla funzione del sistema integrato COMUNI - CNSD – SSCE legato alle attività di rilascio ed uso della CIE.
Negli allegati successivi si riportano le indicazioni, i processi, le strutture ed i compiti che devono essere svolti per l'attuazione del piano della sicurezza dei comuni ai fini dell'emissione delle CIE.
Si precisa che le indicazioni tecnico-organizzative, i vincoli e le tipologie dei documenti descritti, costituiscono il Piano di Sicurezza dei comuni per l'uso e l'emissione delle CIE e rappresentano un requisito imprescindibile per la corretta attuazione del piano stesso.
Il Piano di Sicurezza definitivo ed ogni eventuale modifica procedurale che i Comuni intendano introdurre, dovranno essere esplicitamente approvati dalla Prefettura, a tal fine il Comune è tenuto ad inviare il piano di sicurezza alla Prefettura.

2. Attuazione del Piano della Sicurezza Comunale

Come già descritto, la metodologia individuata è la PDCA, mentre norme per la sicurezza sono quelle definite BS7799.
In base alla metodologia selezionata, il processo di attuazione del piano della sicurezza comunale prevede che il Comune esegua, in modo strettamente sequenziale, le seguenti quattro fasi:

Plan Definizione piano di sicurezza versione alfa
Do Prima implementazione ed attuazione del piano versione alfa
Check Monitoraggio e validazione
Act Manutenzione ed evoluzione, rilascio versione beta del piano.

Tali attività consentono ai Comuni di regidere il primo piano della sicurezza (piano versione alfa) o di verificare la conformità del Piano di sicurezza eventualmente già elaborato, al modello qui descritto.
Il primo piano per la sicurezza è denominato "piano versione alfa" in quanto costituisce un piano provvisorio, destinato ad essere sostituito, dopo i primi sei mesi di applicazione, da un successivo piano di sicurezza, denominato "piano versione beta", calibrato, nelle azioni e negli effetti, sulla specifica realtà tecnico organizzativa di ogni Comune.

2.1. Definizione piano di sicurezza versione alfa

Attività iniziale di questa fase è costituita dalla descrizione dei singoli macroprocessi di emissione ed uso della CIE.
Il Comune deve arricchire, specificare e adeguare le descrizioni e le tabelle relative ai macroprocessi o, attraverso l'uso delle apposite schede fornite, verificare la conformità al modello del piano di sicurezza preesistente.
Risultato dell'attività è costituito dalla descrizione formale, in termini di analisi del rischio, di tutti i processi elementari che compongono i macroprocessi di emissione ed uso della CIE.

A tal fine, si forniscono di seguito le definizioni delle differenti tipologie di processi elementari:

Processo di Front office	è un processo attivato da un operatore al terminale in presenza di un utente che fornisce le informazioni necessarie all'esecuzione del processo;
Processo di Back office di Elaborazione	è un processo che è attivato in base ad informazioni gestite totalmente all'interno dell'organizzazione comunale. Ricadono in questa categoria tutti i processi di estrazione di archivi, aggiornamento massivo di archivi, stampa della CIE, predisposizione dei formati di scambio dati, etc.;
Processo di Back office di Comunicazione	è un processo che attiene esclusivamente all'invio o alla ricezione in rete di dati. Vi rientrano: le richieste di convalida anagrafica, gli invii di variazione dati anagrafici al CNSD, gli invii di richieste di emissione CIE ad SSCE, etc.

Un processo è definito come elementare quando esso ricade in una sola delle classi di processo sopra descritte.

Ai fini della classificazione degli asset (risorse nell'accezione più ampia del termine: tecnologiche, logistiche, umane, economiche, etc.) si utilizza la seguente classificazione:
a) Informazioni
b) Reti
c) Infrastrutture
d) Hardware
e) Software
f) Risorse umane

In questo ed in tutti i successivi capitoli del presente documento si farà riferimento alle due classificazioni appena fornite per i processi elementari e per gli asset coinvolti.

3. Descrizione dei macroprocessi di emissione ed uso CIE

I macroprocessi considerati sono:

- il macroprocesso di caricamento dell'INA
- il macroprocesso di emissione della CIE
- il macroprocesso di uso della CIE.

Al fine di fornire un supporto completo al Comune per la stesura del piano della sicurezza, si riporta di seguito un prospetto sintetico che illustra le principali attività e le relazioni che intercorrono tra queste, per poter attivare i servizi di emissione CIE ai cittadini.

Prospetto sintetico del flusso di attivazione dell'accesso ai domini applicativi del CNSD

Comune
Il sindaco nomina il responsabile comunale per la sicurezza degli accessi al CNSD:
- Comunicazione della nomina del responsabile al Ministero dell'Interno ed alla Prefettura.

Ministero dell'Interno
Predisposizione della "quantità di sicurezza, attivazione e certificazione" del comune:
- Predisposizione firma digitale attribuita al responsabile comunale per la sicurezza degli accessi al CNSD
- Predisposizione strumenti software ed informativi (agenti di monitoraggio e controllo, certificati digitali, tool di servizio) richiesti per l'attivazione della Porta di accesso ai domini applicativi del CNSD e per l'attivazione dei sistemi comunali autorizzati all'accesso ai domini applicativi del CNSD.
- predisposizione supporto tecnologico di archiviazione della "quantità di sicurezza, attivazione e certificazione"

Invio alla Prefettura del supporto tecnologico della "quantità di sicurezza, attivazione e certificazione"

Comune
Redazione Piano di Sicurezza Comunale CIE
- invio alla Prefettura entro il 31-10-2005

Flusso di approvazione piano

Prefettura
Verifica ed approvazione del Piano entro 30 giorni dalla consegna

Ministero dell'Interno
Ricezione ed archiviazione di una copia del Piano, trasmesso al CNSD dalla Prefettura in formato digitale tramite Porta di accesso della Prefettura

Comune
- **Attivazione del piano di sicurezza, entro il 31 12 2005**

Ministero dell'Interno
Riceve comunicazione avvenuta attivazione

Prefettura
Consegna della "quantità di sicurezza, attivazione e certificazione" al responsabile comunale di riferimento:
- custodia in sicurezza fino al momento della consegna
- identificazione sicura del responsabile comunale di riferimento
- consegna della "quantità di sicurezza, attivazione e certificazione" con firma di apposito modulo di presa in carico da parte del comune

Comune
Custodia e gestione della "quantità di sicurezza, attivazione e certificazione":
- verifica al momento della presa in carico della quantità di certificazione e attivazione, sia dell'integrità del supporto che della correttezza dei dati di riferimento in esso contenuti
- custodia in sicurezza

Comune
- Attivazione Porta di accesso ai domini applicativi del CNSD
- attivazione Sistemi comunali per i servizi INA entro il 31 10 2005

Nei paragrafi seguenti si riporta la descrizione dello schema logico di riferimento per i macroprocessi sopra elencati.

3.1. Macroprocesso di caricamento dell'INA

Il macroprocesso di caricamento dell'INA – Indice Nazionale delle Anagrafi, si articola nei seguenti processi:

- Predisposizione Porta di Accesso ai domini Applicativi del CNSD
- Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria
- Primo caricamento dell'Indice Nazionale delle Anagrafi
- Aggiornamento continuo dell'Indice Nazionale delle Anagrafi.

I Comuni accedono a tutti i servizi applicativi, erogati dai sistemi centrali del CNSD, esclusivamente attraverso la propria porta di accesso ai domini applicativi del CNSD, attivata ed abilitata per gli specifici servizi.
Tutte le comunicazioni di rete relative alle richieste di servizio, transitano per la porta di accesso che verifica le quantità di sicurezza utilizzate dal Comune per tali comunicazioni e, tramite Backbone, inserisce le richieste di servizio in un'apposita busta informatica, creata dalla Porta stessa secondo le specifiche del Sistema Pubblico di Connettività (busta di e-gov) e le invia ai sistemi centrali Backbone del CNSD.

Le comunicazioni tra i sistemi comunali e la porta di accesso avvengono secondo il protocollo XML SOAP o Post HTTP XML e devono essere identificate e rese sicure attraverso l'uso delle quantità di sicurezza fornite dal Ministero dell'Interno ai Comuni. Il sistema degli agenti di monitoraggio e allarmi, attivi sulla Porta di Accesso dei Comuni, segnala al CNSD tutte le anomalie (sicurezza, qualità e livelli di servizio) riscontrate nelle fasi di trasmissione dei flussi applicativi e nel funzionamento delle reti comunali.
Presso il CNSD tutte le richieste di servizio provenienti dai Comuni attraverso le porte di accesso, transitano per i sistemi centrali Backbone che verificano la corretta trasmissione delle buste di e-gov e la corrispondenza tra le richieste di servizio pervenute ed i servizi effettivamente registrati presso i sistemi centrali Backbone. In caso positivo, le richieste di servizio sono riportate ai corrispondenti domini applicativi del CNSD per essere trattate e per la formulazione delle relative risposte.

Segue la descrizione dello schema logico di riferimento per il macroprocesso di caricamento INA.

COMUNE
Anagrafe Comunale
Primo caricamento e/o Aggiornamento INA
Porta di Accesso ai domini Applicativi del CNSD
MEF
Anagrafe Tributaria
Richiesta allineamento
Codici Fiscali allineati
CNSD
Richiesta allineamento
Codici Fiscali allineati
Primo caricamento INA
Accesso ai servizi INA
Monitoraggio e allarmi
Sistemi centrali Backbone
Dominio Applicativo INA
Dominio uso CIE
Dominio Monitoraggio e Controllo Emissione CIE
Dominio Emissione CIE

3.2. Macroprocesso di emissione della CIE

Il macroprocesso di emissione della CIE, quando il Comune è stato abilitato all'emissione CIE e quindi ha svolto le attività illustrate nel precedente prospetto sintetico "Flusso di attivazione dei servizi applicativi CNSD", si articola nei seguenti processi:

- Predisposizione delle Postazioni di Emissione.
- Acquisizione delle quantità di sicurezza.
- Acquisizione delle CIE inizializzate dall'Istituto Poligrafico.
- Rilascio CIE ai cittadini:
  - Richiesta emissione CIE.
  - Acquisizione autorizzazione di emissione CIE e stampa della CIE.
  - Attivazione CIE.
  - Rilascio al cittadino.

Le postazioni di emissione di BackOffice, che sono le uniche postazioni di emissione comunali abilitate alle comunicazioni verso i sistemi centrali di emissione CIE, accedono ai servizi di emissione, attivazione e revoca della CIE esclusivamente attraverso la Porta di Accesso ai domini applicativi del CNSD, attivata ed abilitata per tali servizi.
Tutte le comunicazioni di rete relative alle richieste di servizio, transitano per la porta di accesso che verifica le quantità di sicurezza utilizzate dal Comune per tali comunicazioni e, tramite Backbone, inserisce le richieste di servizio in un'apposita busta informatica, creata

dalla Porta stessa secondo le specifiche del Sistema Pubblico di Connettività (busta di e-gov) e le invia ai sistemi centrali Backbone del CNSD.
Il sistema degli agenti di monitoraggio e allarmi, attivi sulla Porta di Accesso dei Comuni, segnala al CNSD tutte le anomalie (sicurezza, qualità e livelli di servizio) riscontrate nelle fasi di trasmissione dei flussi applicativi e nel funzionamento delle reti comunali.
Presso il CNSD tutte le richieste di servizio provenienti dai Comuni attraverso le porte di accesso, transitano per i sistemi centrali Backbone che verificano la corretta trasmissione delle buste di e-gov e la corrispondenza tra le richieste di servizio pervenute ed i servizi effettivamente registrati presso i sistemi centrali Backbone. In caso positivo, le richieste di servizio sono riportate ai corrispondenti domini applicativi del CNSD per essere trattate e per la formulazione delle relative risposte.

Nel caso in cui le funzioni di pertinenza dei Comuni per i procedimenti di Back office dovessero essere esercitate in centri di allestimento periferici per la stampa della CIE, tutti i flussi relativi ai processi di emissione CIE provenienti dalle postazioni di emissione CIE di "Front office" dovranno essere indirizzati al centro di allestimento periferico di riferimento. L'accesso al CNSD e, attraverso questo, ai servizi di SSCE, avviene tramite una specifica Porta di Accesso ai domini applicativi del CNSD che deve essere situata, registrata ed abilitata presso lo stesso centro di allestimento.

Segue la descrizione dello schema logico di riferimento.

COMUNE

Uno o più punti di Front Office di acquisizione dati anagrafici e biometrici

Uno o più punti di Front Office per rilascio CIE ai cittadini

Emissione CIE al cittadino

Attivazione CIE

Richiesta Emissione CIE

Uno o più punti di Back Office per allestimento e stampa CIE

Flussi CIE

Porta di Accesso ai domini Applicativi del CNSD

Richiesta emissione CIE

Autorizzazione emissione CIE

Attivazione CIE

monitoraggio ed allarmi

SSCE

Richiesta emissione CIE

Autorizzazione emissione CIE

Attivazione CIE

Aggiornamento archivio CIE-COMUNI

monitoraggio ed allarmi

CNSD

Sistemi centrali Backbone

Dominio Applicativo INA

Dominio uso CIE

Dominio Monitoraggio e Controllo Emissione CIE

Convalida anagrafica

Dominio Emissione CIE

Archivio CIE Comuni

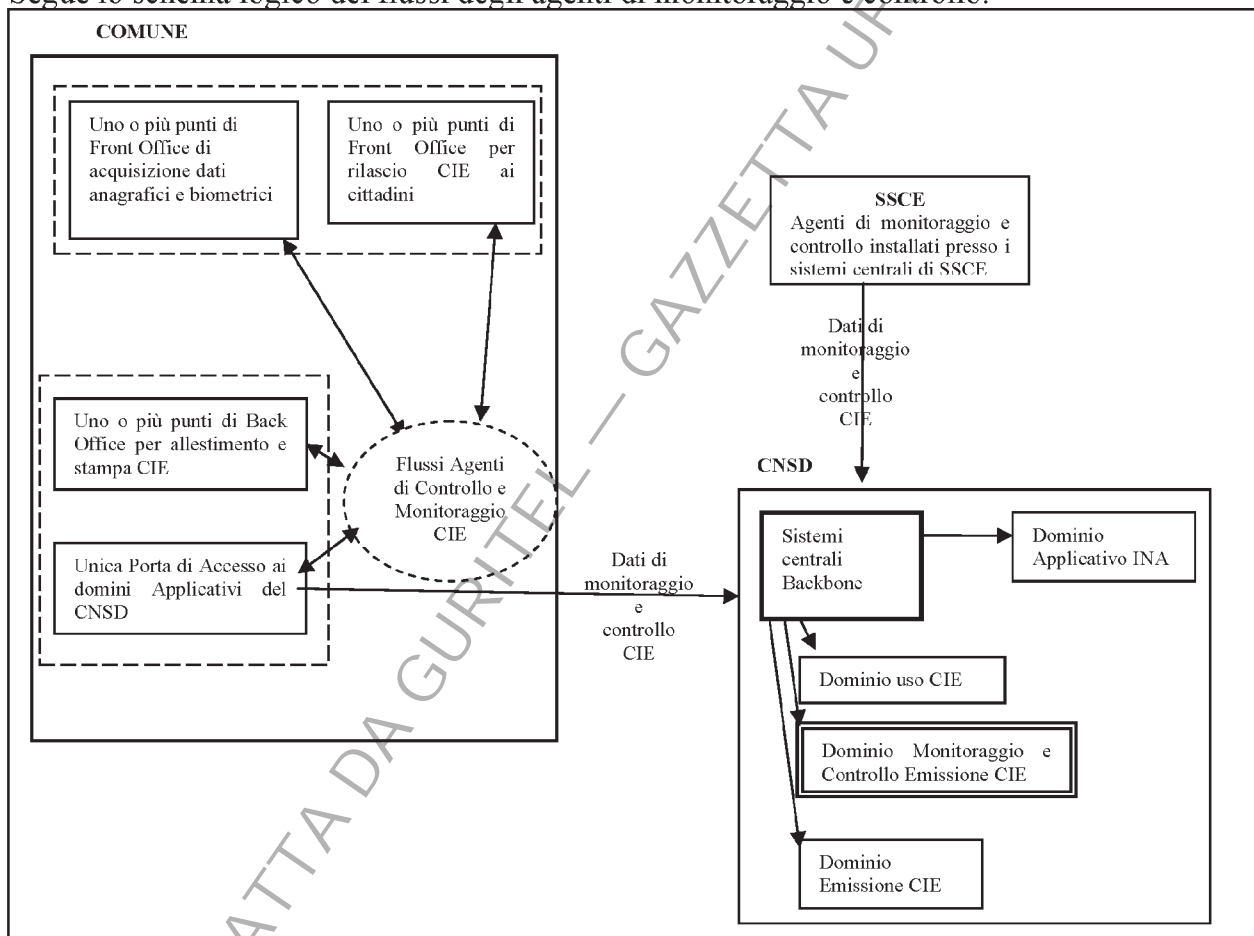
Rispetto allo schema precedente si evidenzia come il punto di emissione CIE comunale si suddivide nelle seguenti entità logiche:

- anagrafe comunale
- punti di Front Office:
  - Uno o più punti di acquisizione dati anagrafici e biometrici
  - Uno o più punti per rilascio CIE ai cittadini
- punti di Back Office:
  - Uno o più punti per allestimento e stampa CIE
- porta di accesso ai domini applicativi del CNSD:
  - Un unico punto di accesso ai domini applicativi del CNSD

Il modello organizzativo sul quale si cala l'architettura logica esposta, può variare in base alla realtà organizzativa, logistica e tecnica dei singoli comuni. In particolare si evidenzia che:

- può variare il numero dei punti sia di front office per l'acquisizione dei dati ed il rilascio delle CIE, che di back office per l'allestimento e la stampa delle CIE;
- tutte le comunicazioni con il CNSD devono passare per la Porta di accesso del Comune ai domini applicativi del CNSD.

Oltre ai flussi descritti in precedenza, nell'ambito dell'emissione CIE sono presenti anche i flussi di controllo e monitoraggio del sistema di emissione CIE. Tali flussi sono gestiti dagli Agenti di Controllo e dagli agenti di Monitoraggio, che devono essere correttamente installati e configurati nelle postazioni CIE (front office e back office). Tali agenti controllano e certificano lo stato di funzionamento ed operatività delle postazioni di front office, di back office e delle porte di accesso ai domini applicativi del CNSD. Al fine di ottenere l'autorizzazione all'emissione di CIE, il Comune è tenuto ad adottare le opportune politiche di sicurezza e le relative procedure operative per la configurazione della rete e per la gestione in sicurezza delle postazioni.

Segue lo schema logico dei flussi degli agenti di monitoraggio e controllo.

Nel caso le funzioni di pertinenza dei Comuni per i procedimenti di Back office di stampa della CIE, vengano esercitate presso centri periferici di allestimento, tutti i flussi relativi ai processi di emissione CIE provenienti dalle postazioni di emissione CIE di "Front office" devono essere indirizzati al centro di allestimento di riferimento. L'accesso ai servizi del CNSD e, attraverso questo, di SSCE, avviene tramite la porta di accesso ai servizi applicativi del CNSD situata presso il centro di allestimento periferico.

3.3. Macroprocesso di uso della CIE

Il macroprocesso di uso della CIE, riguarda l'uso della CIE da parte di un cittadino (cui è stata rilasciata la CIE da un Comune) che accede ad un servizio comunale in rete. Il macroprocesso si articola nei seguenti processi e sottoprocessi elementari:

- Abilitazione di una postazione di lavoro all'identificazione in rete della CIE
- Abilitazione di un server comunale per l'identificazione in rete dei cittadini tramite CIE

I Comuni accedono a tutti i servizi applicativi, erogati dai sistemi centrali del CNSD, esclusivamente attraverso la propria porta di accesso ai domini applicativi del CNSD, attivata ed abilitata per gli specifici servizi.
Tutte le comunicazioni di rete relative alle richieste di servizio, transitano per la porta di accesso che verifica le quantità di sicurezza utilizzate dal Comune per tali comunicazioni e, tramite Backbone, inserisce le richieste di servizio in un'apposita busta informatica, creata dalla Porta stessa secondo le specifiche del Sistema Pubblico di Connettività (busta di e-gov) e le invia ai sistemi centrali Backbone del CNSD.

Le comunicazioni tra i sistemi comunali e la porta di accesso avvengono secondo il protocollo XML SOAP o Post HTTP XML e devono essere identificate e rese sicure attraverso l'uso delle quantità di sicurezza fornite dal Ministero dell'Interno ai Comuni. Il sistema degli agenti di monitoraggio e allarmi, attivi sulla Porta di Accesso dei Comuni, segnala al CNSD tutte le anomalie (sicurezza, qualità e livelli di servizio) riscontrate nelle fasi di trasmissione dei flussi applicativi e nel funzionamento delle reti comunali.
Presso il CNSD tutte le richieste di servizio provenienti dai Comuni attraverso le porte di accesso, transitano per i sistemi centrali Backbone che verificano la corretta trasmissione delle buste di e-gov e la corrispondenza tra le richieste di servizio pervenute ed i servizi effettivamente registrati presso i sistemi centrali Backbone. In caso positivo, le richieste di servizio sono riportate ai corrispondenti domini applicativi del CNSD per essere trattate e per la formulazione delle relative risposte.

Segue la descrizione dello schema logico di riferimento per l'uso della CIE come strumento di accesso ai servizi di rete.

Utenti

COMUNE

Uno o più servizi applicativi Comunali

Porta di Accesso ai domini Applicativi del CNSD

Verifica validità certificato CIE

Associazione id. carta e Codice Fiscale

Convalida anagrafica CIE

CNSD

Servizi centrali backbone

Dominio Applicativo INA

Servizio distribuito di convalida dei certificati

Dominio uso CIE

Dominio Monitoraggio e Controllo Emissione CIE

White List CIE (lista delle carte valide)

Dominio Emissione CIE

4. Politiche di sicurezza

Di seguito sono presentate le politiche di sicurezza che il Comune deve adottare, in conformità alle direttive emanate dal Ministero dell'Interno in quest'ambito ed agli standard internazionali in tema di sicurezza.

Dallo standard BS7799 si ricavano le seguenti dieci categorie:

1. Politica e standard di sicurezza;
2. Organizzazione per la sicurezza;
3. Controllo e classificazione delle risorse;
4. Sicurezza del personale;
5. Sicurezza materiale e ambientale;
6. Gestione operativa e comunicazione;
7. Controllo degli accessi;
8. Sviluppo e manutenzione dei sistemi;
9. Gestione della business continuity;
10. Conformità.

In tale insieme vanno selezionate, attraverso le attività di analisi del rischio, quelle linee guida che soddisfano le esigenze di sicurezza del Comune. Le linee guida prescelte vanno così a costituire un insieme di controlli di sicurezza che il Comune si impegna ad attuare.

Tali controlli devono essere realizzati attraverso:

- meccanismi hardware o software (sistemi di autenticazione tramite password, token card, smart card, prodotti per la protezione crittografica dei dati, firewall, etc.);
- sistemi anti intrusione, telecamere, tornelli, casseforti, contenitori ignifughi, etc.;
- la creazione di apposite strutture o funzioni all'interno dell'organizzazione e la definizione di procedure organizzative (ad esempio l'istituzione di un forum per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di formazione periodica del personale, le procedure per l'accettazione di ospiti all'interno dell'organizzazione, ecc.).

Nei paragrafi successivi sono analizzati in dettaglio i dieci punti sopra elencati, e definite le principali politiche di sicurezza che il Comune deve attuare.

4.1. Politica e standard di sicurezza (Security Policy)

L'obiettivo è quello di dare direttive per la gestione delle informazioni di sicurezza.
Il Comune deve attenersi ai seguenti principi generali:

a) Tutti gli accessi ai servizi applicativi del CNSD devono avvenire tramite la porta di accesso del Comune ai domini applicativi del CNSD;
b) Tutte le informazioni (dati, documenti, archivi, …) devono essere protette e mantenute;
c) Per la riservatezza dei contenuti scambiati, la sicurezza deve essere garantita anche a livello delle reti di comunicazioni dati;
d) Deve essere gestita la sicurezza sia di tutti gli apparati inerenti la struttura comunale di emissione ed uso della CIE, sia del materiale di consumo considerato sensibile ai fini della sicurezza;
e) Tutte le registrazioni devono essere oggetto di monitoraggio costante (manuale o automatico);
f) Devono essere predisposte adeguate misure di sicurezza per l'accesso ai locali che ospitano le postazioni di front office, back office e la Porta di accesso al CNSD, nonché tutto il materiale impiegato nei processi di rilascio della CIE;
g) Ogni eventuale incidente o evento straordinario che possa pregiudicare la sicurezza deve essere oggetto di analisi e di rapporto scritto;
h) La Porta di accesso ai domini applicativi del CNSD e le postazioni di emissione CIE, sia di back office che di front office, devono essere utilizzati ai soli fini del rilascio ed uso della CIE e per l'accesso ai servizi del CNSD;
i) Tutti i progetti di nuove applicazioni/servizi devono essere inseriti nel piano per la sicurezza;
j) Tutte le modifiche, eventualmente apportate ai processi organizzativi interni al Comune, devono essere inserite nel Piano per la Sicurezza che va nuovamente trasmesso alla Prefettura per l'approvazione.
k) Per tutti i processi o macroprocessi CIE, deve essere individuato un responsabile di riferimento.
l) Nel caso in cui si dovessero utilizzare eventuali centri di allestimenti periferici per l'allestimento e la stampa delle CIE, devono essere gestiti in sicurezza tutti i possibili trasferimenti di CIE, di quantità di sicurezza e, in generale, di tutte le componenti e informazioni sensibili;

m) I servizi di monitoraggio degli accessi devono essere estesi a tutti gli apparati di front office e back office ed alla Porte di Accesso ai domini Applicativi del CNSD. In particolare si richiede:
   - Identificazione di ogni punto (back office, front office, Porta di accesso ai domini applicativi del CNSD) inerente l'uso e l'emissione della CIE;
   - certificazione delle operazioni, effettuata dagli agenti di monitoraggio e controllo installati sulle postazioni;
   - tracciatura delle operazioni effettuate con conseguente valutazione del livello di qualità dei servizi CIE, effettuata dagli agenti di monitoraggio e controllo installati sulle postazioni.

Inoltre, relativamente alle problematiche di sicurezza inerenti l'emissione e l'uso della CIE, devono essere stabilite le seguenti responsabilità:
- responsabilità di chi definisce, aggiorna ed approva le regole di sicurezza del Comune in ambito CIE;
- responsabilità di chi fornisce le configurazioni e/o gli aggiornamenti che devono essere implementati nei sistemi di sicurezza (firewall, routing, switch, Porta di accesso ai domini applicativi del CNSD, postazioni di front office, postazioni di back office…) per assicurare il mantenimento dei livelli di sicurezza del Comune.

Deve essere inoltre individuato:
- la persona fisica che effettua la gestione operativa dell'infrastruttura di sicurezza, sia relativamente agli applicativi software sia relativamente ai sistemi di calcolo su cui i medesimi sono installati;
- la persona fisica chi effettua la gestione di tutti gli altri sistemi presenti nel Comune e comunque attinenti all'emissione ed all'uso della CIE;
- la persona fisica effettua la manutenzione di tutti gli apparati attinenti all'emissione ed all'uso della CIE presenti presso il Comune.

4.2. Organizzazione per la sicurezza (Security Organization)

Il Comune deve definire e costituire un settore preposto a sovrintendere e controllare i processi e le attività legate alla sicurezza dell'infrastruttura di emissione ed utilizzo della CIE.

4.3. Classificazione e Controllo delle risorse (Asset Classification and Control)

Il Comune deve raccogliere e classificare informazioni su tali risorse. In particolare le risorse da considerare sono:

- Sistemi informativi;
- Sistemi di rete tra le varie sedi (intranet, internet);
- Postazioni di lavoro;

- Postazioni di Front Office;
- Postazioni di Back Office;
- Porta di accesso ai domini applicativi del CNSD;
- Punti di accesso multimediali aperti al pubblico.

4.3.1. Inventario delle risorse

Gli eventuali trasferimenti di beni in entrata ed uscita devono essere autorizzati dal responsabile del Comune.
Tutte le risorse del Comune devono essere inventariate.

Per ogni risorsa deve essere dichiarato:

- l'area/servizio a cui è assegnata la risorsa;
- il responsabile della risorsa;
- le autorizzazioni di accesso e di utilizzo della risorsa.

4.4. Sicurezza del personale (Personnel Security)

Gli obiettivi sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture comunali;
- accertarsi che il personale addetto sia stato informato sui possibili rischi relativi alla sicurezza delle informazioni.

4.5. Sicurezza materiale e ambientale (Physical and Environmental Security)

Gli obiettivi sono:

- impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni;
- impedire la perdita o il danneggiamento dei dati necessari alla corretta esecuzione dei processi di emissione ed uso della CIE;
- impedire l'interruzione delle attività.

4.6. Gestione dei sistemi e delle reti (Computer and Network Management)

Gli obiettivi sono:

- assicurare il corretto e sicuro funzionamento sistemi di elaborazione e delle reti;
- minimizzare il rischio di guasti dei sistemi;
- proteggere l'integrità del software di base e delle informazioni;
- assicurare la disponibilità dei processi di elaborazione dell'informazione e di comunicazione;

- garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di rete;
- evitare la perdita, modifica o uso improprio delle informazioni scambiate in rete.

Tutti gli accessi ai servizi INA ed ai servizi di emissione ed uso della CIE, devono avvenire nell'ambito delle seguenti infrastrutture di sicurezza:

- Backbone di Sicurezza del CNSD e Porta di accesso ai domini applicativi del CNSD;
- Sistema di Sicurezza del Circuito di Emissione delle carte di identità e dei documenti di identità elettronici.

In particolare, la porta di accesso ai domini applicativi del CNSD rappresenta il punto di presa in carico delle comunicazioni provenienti dal Comune (aggiornamento INA, flussi di emissione della CIE, altri servizi anagrafici) e del loro successivo inoltro al CNSD. Tale porta di accesso certifica il punto di origine delle comunicazioni, individuando univocamente il Comune che comunica con il CNSD: **tutte le comunicazioni devono quindi avvenire esclusivamente tramite la porta di accesso del Comune ai domini applicativi del CNSD**.
Ciascun Comune deve registrare presso il Ministero dell'Interno la porta di accesso ai domini applicativi del CNSD che utilizza per le comunicazioni con il CNSD.

In conformità con le infrastrutture di sicurezza sopra elencate, nel rispetto della normativa anagrafica e delle prerogative del Ministero dell'Interno per quanto riguarda la vigilanza anagrafica, il Comune deve prevedere:

- identificazione delle postazioni di lavoro che si collegano ai servizi INA e ai servizi di emissione della CIE;
- sistema di documentazione, monitoraggio ed allarmi dei servizi, che fornisca in modo preciso ed inequivocabile tutte le informazioni necessarie a descrivere le anomalie di sicurezza e ad individuare le responsabilità (svolta dagli agenti di monitoraggio e controllo installati sulle postazioni);
- sistema di allarme inerente accessi ed usi impropri dei servizi.

Gli accessi in rete ai servizi del CNSD devono avvenire nel pieno rispetto delle regole riportate nel documento "*Regole tecniche e di sicurezza per l'accesso ai domini applicativi del CNSD*".

4.7. Controllo degli accessi (System Access Control)

Gli obiettivi di questa sezione sono:

- controllare l'accesso alle informazioni;
- prevenire l'accesso non autorizzato alle informazioni;
- assicurare la protezione dei servizi in rete;
- prevenire l'accesso non autorizzato alle postazioni di emissione sia di front office che di back office ed alla Porta di accesso ai domini applicativi del CNSD;
- rilevare attività non autorizzate;

- garantire la sicurezza delle informazioni quando sono utilizzate da eventuali postazioni mobili in rete;
- garantire un adeguato controllo degli accessi ai locali comunali che ospitano le postazioni di front office, di back office, la Porta di accesso al CNSD, nonché tutto il materiale impiegato nei processi di rilascio della CIE.

4.8. Sviluppo e manutenzione dei sistemi (System Development and Maintenance)

Gli obiettivi sono:

- garantire che le regole di sicurezza siano realmente attuate nei sistemi informatici in esercizio;
- assicurare che la conduzione dei progetti informatici e le relative attività di supporto siano eseguite secondo le regole riportate nel presente piano di sicurezza.

Tutti i progetti di nuove applicazioni/servizi devono essere inseriti nel Piano per la Sicurezza.

4.9. Gestione della continuità del servizio (Business Continuity Management)

Gli obiettivi di questa sezione sono di contrastare le interruzioni delle attività di servizio e dei processi di servizio critici, causati da malfunzionamenti o da eventuali avvenimenti straordinari. Infatti: "**Lo scopo del *Business Continuity Management* è garantire la continuità dei processi dell'Organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni**" (Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni del CNIPA - documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" – marzo 2004).

Per una corretta gestione del governo delle informazioni i sistemi devono garantire la continuità dei servizi.
Di seguito è sintetizzata una classificazione di eventi straordinari:

1. Un disastro di primo livello su un ufficio può causare, in alcuni casi, la parziale ma non completa distruzione delle operazioni svolte giornalmente. La situazione può essere risolta usando personale dell'ufficio stesso ed effettuando localmente attività di ripristino.

2. Un disastro di secondo livello può coinvolgere diversi uffici. Le operazioni di routine possono essere distrutte ed i processi critici dovranno essere eseguiti in altri uffici. Il personale dell'ufficio potrebbe avvalersi dell'assistenza di soggetti esterni. Il coordinamento delle

persone avviene attraverso un centro di operazioni di emergenza appositamente costituito dal Comune.

3. Un disastro di terzo livello può coprire una vastissima zona, ad esempio una regione; tipici esempi di questi eventi straordinari sono: inondazioni, terremoti o uragani. In questo caso sono richieste risorse esterne ed assistenza, ma il ripristino completo può richiedere settimane o mesi. Generalmente un disastro di questo livello comporta il blocco dell'operatività dei sistemi.

I sistemi devono essere classificati secondo le definizioni seguenti:

Critici Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

Vitali Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici; conseguentemente il costo di un'interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

Delicati Queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

Non-critici Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un costo modesto, o nullo, e si richiede un limitato sforzo di riattivazione quando il sistema viene ripristinato.

A fronte delle precedenti considerazioni, in caso di eventuali avvenimenti straordinari, devono essere rispettate le seguenti regole:

- le procedure applicative, il software di sistema e gli archivi che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente;
- il piano d'emergenza deve prevedere il ripristino di tutte le funzioni e non solo i servizi informatici centrali;
- per assicurare la continuità dei servizi devono essere valutate le strategie di ripristino più opportune quali:
  - siti alternativi;
  - metodi di back up;
  - sostituzione dei sistemi hardware di elaborazione;

- ruoli e responsabilità dei gruppi tecnici di lavoro.

4.10. Conformità (Compliance)

Gli obiettivi sono:

- garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari o contrattuali e di qualsiasi requisito di sicurezza;
- garantire il rispetto di tutte le direttive del Ministero dell'Interno;
- assicurare la conformità dei sistemi con i criteri e gli standard di sicurezza nazionali ed internazionali.

Allegato 3
Redazione del piano di sicurezza versione alfa: definizione struttura di riferimento, analisi e classificazione delle procedure operative

1. Introduzione

Questo allegato illustra e fornisce tutti gli strumenti necessari alla redazione del primo piano della sicurezza (piano versione alfa).

Il Comune deve specificare, adeguandole alla propria realtà tecnica ed organizzativa, le descrizioni e le tabelle relative sia alla struttura organizzativa, logistica e tecnologica, sia ai macroprocessi, processi ed attività elementari inerenti all'emissione ed all'uso della CIE.

Tale attività mira ad ottenere la descrizione formale, in termini di analisi del rischio, di tutti i singoli processi elementari che compongono i macroprocessi legati all'emissione ed all'uso della CIE ed una rappresentazione di insieme della struttura organizzativa, logistica e tecnologica del Comune.
È pertanto necessario procedere all'ulteriore scomposizione dei processi individuati, qualora essi non si identifichino interamente in una delle tre tipologie di processo elementare precedentemente descritte.

È stata individuata la seguente classificazione degli asset:

a) Informazioni
b) Reti
c) Infrastrutture
d) Hardware
e) Software
f) Risorse umane.

Tutti gli asset devono quindi essere ricondotti ad elementi di questa classificazione. Nel caso in cui un Comune dovesse individuare nella redazione del suo Piano, una nuova classe, sufficientemente descrittiva della realtà comunale, deve inserirla e, per ogni attività/processo elementare già individuato in questo documento, deve associare gli asset appartenenti a questa nuova classe.

Si fa rilevare, inoltre, che, nel seguito, per ogni attività/processo elementare individuato, sono stati elencati un insieme di "controlli" che devono essere attuati, secondo modalità scelte dal Comune in base alla sua struttura tecnologica ed organizzativa ed un insieme di "asset" relativi alle singole attività/processi elementari.

2. Come si utilizza questo allegato

Quest'allegato consente al Comune, che deve specializzarlo, arricchirlo ed adeguarlo alla propria realtà tecnico-organizzativa, di redigere il proprio piano di sicurezza o, se l'ha già redatto, di verificarlo attraverso la scheda di verifica fornita.

Si evidenzia che per tutti i processi di seguito illustrati il Comune è tenuto a valutare, tra gli altri, tutti gli aspetti di sicurezza inerenti:

- **copie di sicurezza dei dati,**
- **continuità del servizio anche in caso di incidenti di sicurezza o eventi straordinari,**
- **gestione degli accessi.**

Al termine, si otterrà un documento, analogo a questo allegato, che costituisce la base per la redazione del piano per la sicurezza.

2.1. Descrizione della struttura organizzativa, logistica e tecnologica di riferimento per l'emissione e l'uso della CIE

L'obiettivo è di descrivere, offrendo una visione di insieme, la struttura comunale organizzativa, logistica e tecnica di riferimento per l'emissione e l'uso della CIE. Gli stessi elementi qui riportati devono essere indicati anche nell'ambito della descrizione dettagliata delle procedure.

Il Comune, in base alla propria realtà organizzativa e tecnica, è tenuto a fornire le seguenti informazioni su:
- configurazione del Comune (denominazione, provincia, etc.);
- uffici e servizi;
- ruoli e figure professionali previste per l'emissione e l'uso della CIE;
- dispositivi installati;
- Altre informazioni sensibili per la sicurezza;
  - infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza CIE;
  - Ubicazione dei servizi e degli uffici CIE negli immobili comunali;
  - Elenco del personale e sua assegnazione agli uffici.

2.2. Descrizione dei macroprocessi di emissione ed uso CIE

I processi cui si fa riferimento e che sono descritti, coinvolgono un insieme di entità ben distinte: i Comuni, i cittadini, i fornitori dei servizi informatici del Comune, il CNSD, il SSCE.

I macroprocessi considerati sono:

- il macroprocesso di caricamento dell'INA
- il macroprocesso di emissione della CIE
- il macroprocesso di uso della CIE.

3. Struttura generale, modalità organizzativa e struttura logistica di riferimento per l'emissione e l'uso della CIE

3.1. Presentazione del Comune

Indicare:

- la denominazione,
- la provincia di riferimento,
- il numero degli abitanti,
- il numero dei cittadini ultraquindicenni,
- la sede principale del Comune.

3.2. Descrizione dei Macroprocessi di emissione ed uso della CIE

L'indicazione puntuale di tutti gli elementi previsti nelle apposite schede informative, indicate nei capitoli successivi, consentirà ai Comuni di rappresentare in modo fedele i tre macroprocessi di emissione CIE:

- macroprocesso di caricamento dell'INA
- macroprocesso di emissione della CIE
- macroprocesso di uso della CIE.

3.3. Descrizione degli uffici e dei servizi

In riferimento ai tre macroprocessi di emissione ed uso della CIE ("Caricamento dell'INA", "Emissione della CIE" e "Uso della CIE") il Comune è tenuto a descrivere la propria struttura organizzativa, con riferimento a:

- Settore/area: il Comune è diviso in più settori/aree. Ogni settore/area identifica una macro area con un proprio responsabile di riferimento.
- Servizi: nell'ambito di un settore/area sono erogati più servizi. Per ogni servizio è previsto un responsabile di riferimento.
- Uffici: un servizio, a sua volta, può essere diviso in più uffici addetti a mansioni differenti o, comunque, alla copertura di diverse aree territoriali del Comune (per esempio circoscrizioni). Per i comuni medio/piccoli è possibile che l'ufficio corrisponda al servizio stesso. In tal caso riportare sotto la voce dell'ufficio la stessa voce del servizio.

È inoltre richiesta la descrizione delle principali attività svolte dall'ufficio nell'ambito dei tre macroprocessi CIE.

Il Comune deve quindi provvedere al corretto riempimento della seguente tabella:

<table>
<tr><td>Settore/area</td><td colspan="5"></td></tr>
<tr><td>Descrizione Settore/area</td><td colspan="5"></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>Servizio</td><td>Descrizione servizio</td><td>Ufficio</td><td>Principali attività svolte</td><td>Tipologia di attività</td><td>Descrizione Infrastruttura logistica</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Compilare la tabella/modulo in osservanza delle seguenti indicazioni:

- *Settore/area*: riportare la denominazione del settore o area di riferimento per il macroprocesso CIE;
- *Descrizione settore/area*: riportare una breve descrizione dei principali obiettivi del settore/area
- *Servizio*: riportare la denominazione del servizio inerente il macroprocesso CIE di riferimento
- *Descrizione Servizio*: riportare una descrizione sintetica dei principali obiettivi del servizio
- *Ufficio*: riportare la denominazione dell'ufficio. Per i comuni medio/piccoli è possibile che l'ufficio corrisponda al servizio stesso. In tal caso riportare sotto la voce dell'ufficio la stessa voce del servizio
- *Principali attività svolte*: riportare una descrizione sintetica delle competenze, ovvero delle principali attività svolte dall'ufficio nell'ambito dei macroprocessi CIE;
- *Tipologia di attività*: a seconda della tipologia di attività svolta, assegnare una o più delle denominazioni di processo che seguono:

    - *Processo di "Front office"*: attività svolte in presenza di un utente che fornisce le informazioni necessarie all'esecuzione del processo;

    - *Processo di "Back office di Elaborazione":* servizi svolti all'interno dell'organizzazione comunale, senza necessità di acquisire informazioni "in linea" da utenti allo sportello. Ricadono in questi servizi tutti i processi informatici di estrazione di archivi, aggiornamento di archivi, stampa della CIE, predisposizione dei formati di invio dati e tutti gli altri processi di elaborazione;

    - *Processo di "Back office di Comunicazione":* servizi relativi esclusivamente all'invio o alla ricezione di flussi informativi. I presenti servizi si possono distinguere, per esempio, in: convalida anagrafica, invio variazione dati anagrafici al CNSD, richieste di emissione CIE e qualsiasi altro flusso di comunicazione.

- *Descrizione Infrastruttura logistica*: riportare la descrizione sintetica dell'infrastruttura logistica dell'ufficio. In tale campo riportare la seguente tipologia di informazione:
  - indicare se è previsto o meno un ambiente dedicato esclusivamente per tale ufficio
  - indicare se l'ufficio ha un unico ambiente o se è distribuito su più immobili o comunque su più ambienti
  - indicare se il locale è aperto al pubblico.

3.4. Ruoli e figure professionali per l'emissione e l'uso della CIE

Con riferimento agli uffici descritti nel precedente paragrafo, il Comune deve indicare i ruoli e le figure professionali delle unità di personale addette agli stessi. Si evidenzia che nell'ambito della struttura comunale per l'emissione e l'uso della CIE, il Comune è tenuto **obbligatoriamente** a prevedere almeno i seguenti responsabili:

- *Responsabile comunale per la sicurezza degli accessi al CNSD*: responsabile dell'attivazione e della corretta gestione della Porta di Accesso ai Domini Applicativi del CNSD, nonché e dell'attivazione dei sistemi comunali autorizzati all'accesso ai servizi applicativi del CNSD. Nell'ambito delle sue attività, il Responsabile comunale per la sicurezza degli accessi al CNSD è altresì responsabile della custodia in sicurezza delle "Quantità di sicurezza, attivazione e certificazione"
- *Responsabile della sicurezza CIE*: propone e definisce le regole di sicurezza del Comune. Per ogni macroprocesso CIE deve essere definito il responsabile di sicurezza. In base alla realtà comunale, lo stesso responsabile può essere di riferimento per tutti e tre i macroprocessi CIE.
- *Responsabile della custodia delle Quantità di Sicurezza* (certificati per emissione CIE): responsabile della custodia e gestione delle Quantità di Sicurezza. Il responsabile è tenuto a denunciare al responsabile CIE ogni tentativo di accesso non autorizzato. Tale responsabile deve verificare l'integrità del luogo di custodia e di tutte le relative credenziali di accesso. L'accesso alle Quantità di Sicurezza deve essere consentito al solo personale autorizzato. Ogni accesso autorizzato deve essere registrato riportando almeno le seguenti informazioni:
  - Data ed ora della presa in consegna;
  - Nominativo del personale a cui è stata consegnata la Quantità di Sicurezza;
  - Data ed ora della restituzione.
- *Responsabile caricamento INA*: effettua la gestione operativa dell'infrastruttura inerente al macroprocesso CIE di caricamento dell'INA;
- *Responsabile di emissione della CIE*: effettua la gestione operativa dell'infrastruttura inerente al macroprocesso di emissione CIE;
- *Responsabile della sicurezza dei dati*: responsabile dei backup dei dati relativi ai tre macroprocessi CIE. Tale responsabile deve garantire l'integrità e la custodia di tutte le copie di sicurezza, consentendone l'accesso al solo personale autorizzato;
- *Responsabile delle postazioni di emissione sia di front office che di back office*: gestisce e coordina le attività di configurazione/aggiornamento che devono essere svolte sulle postazioni di front office e Back office CIE;

- *Responsabile della Porta di accesso ai domini applicativi del CNSD*: gestisce e coordina le attività di configurazione/aggiornamento che devono essere svolte sulla Porta di accesso ai domini applicativi del CNSD;
- *Responsabile della rete*: gestisce e coordina le attività di configurazione/aggiornamento che devono essere svolte su tutti i sistemi inerenti la rete comunale (router, firewall, Proxy,;
- *Responsabile dei servizi tecnici*: gestisce e coordina le attività di configurazione/aggiornamento che devono essere svolte in tutti gli altri sistemi informatici presenti nel Comune e comunque attinenti all'emissione ed all'uso della CIE;
- *Responsabile delle verifiche e delle ispezioni (auditing)*: pianifica, gestisce e coordina tutte le attività di controllo e verifica della corretta attuazione del piano di sicurezza;
- *Responsabile della manutenzione*: gestisce e coordina tutte le attività di manutenzione delle risorse tecnologiche impiegate nei processi di emissione ed uso della CIE.

Sempre in riferimento alla propria realtà, il Comune è quindi tenuto al corretto riempimento della presente tabella.

Ufficio	Ruolo	Descrizione ruolo	Figura Professionale	Responsabilità

Compilare la tabella/modulo in osservanza alle seguenti indicazioni:

- *Ufficio:* riportare tutti gli uffici descritti nel precedente paragrafo. Qualora necessario indicare anche il settore/area ed il servizio di riferimento.
- *Ruolo:* in riferimento agli adempimenti dell'ufficio, elencare tutti i ruoli richiesti. Inoltre riportare tutti i responsabili di riferimento.
- *Descrizione ruolo:* riportare una breve descrizione del ruolo indicando le mansioni dello stesso.
- *Figura professionale:* indicare le figure professionali richieste/previste per la copertura del ruolo
- *Responsabilità*: indicare la responsabilità prevista per ciascun ruolo.

Ad esempio, con riferimento alla manutenzione delle postazioni di emissione potrebbe essere inserito:

Ufficio	Ruolo	Descrizione ruolo	Figura Professionale	Responsabilità
Emissione CIE	Responsabile Postazioni di Emissione	Deve verificare la conformità delle Postazioni di emissione sia in riferimento allo stato funzionale sia alle direttive del Ministero	Responsabile tecnico	In caso di malfunzionamenti o guasti delle postazioni di emissione, la manutenzione è a cura del fornitore/gestore della postazione

		dell'Interno (accessi, configurazione, …)		sotto la supervisione del Responsabile delle Postazioni di Emissione

3.5. Descrizione dei dispositivi installati

Descrivere i dispositivi installati evidenziando almeno le seguenti tipologie:
- Postazioni di Emissione CIE di Front Office
- Postazioni di Emissione CIE di Back Office per l'allestimento e stampa delle CIE
- Porta di accesso ai domini applicativi del CNSD
- Altre postazioni di lavoro
- Dispositivi server e di archiviazione dei dati
- Dispositivi di rete
- Sistemi crittografici o altri sistemi di sicurezza
- Dispositivi di backup
- Dispositivi di monitoraggio.

Con riferimento alla classificazione sopra esposta, per ogni macroprocesso CIE, il Comune in base alla propria realtà tecnica è tenuto alla corretta compilazione della seguente tabella:

Tipologia	Dispositivo	Quantità	Caratteristiche tecniche	Descrizione della configurazione	Assegnazione	Responsabile	Personale autorizzato all'accesso

Compilare la tabella/modulo secondo le seguenti indicazioni:
- *Tipologia*: indicare la tipologia del dispositivo facendo riferimento alle denominazioni di seguito riportate:
  - Postazioni di Emissione CIE di Front Office
  - Postazioni di Emissione CIE di Back Office per l'allestimento e stampa delle CIE
  - Porta di accesso ai domini applicativi del CNSD
  - Altre postazioni di lavoro
  - Dispositivi server e di archiviazione dei dati
  - Dispositivi di rete
  - Sistemi crittografici o altri sistemi di sicurezza
  - Dispositivi di backup
  - Dispositivi di monitoraggio.
  - Altro

- *Dispositivo*: riportare una descrizione del dispositivo (per esempio per un dispositivo di rete evidenziare se trattasi di firewall, switch, proxy o altro)
- *Quantità*: riportare il numero di dispositivi presenti
- *Caratteristiche tecniche*: riportare una breve descrizione delle principali caratteristiche tecniche del dispositivo
- *Descrizione della configurazione*: riportare una breve descrizione della configurazione dei dispositivi in riferimento alle politiche di sicurezza (accessi logici, collegamento su rete, condivisione risorse e quanto altro)
- *Assegnazione*: indicare a quale ufficio, servizio o settore è assegnato il dispositivo installato.
- *Responsabile*: riportare il responsabile della risorsa indicando il ruolo e, qualora necessario, il relativo ufficio di riferimento;
- *Personale autorizzato all'accesso*: riportare l'elenco delle figure professionali abilitate ad accedere al dispositivo installato, evidenziandone il tipo di accesso (per esempio per manutenzione, per backup, per lavoro ordinario e/o quanto altro ancora)

3.6. Altre Informazioni sensibili per la sicurezza

Nella redazione del Piano di Sicurezza, il Comune è tenuto alla redazione delle seguenti informazioni:

- Descrizione dell'infrastruttura di sicurezza per ciascun immobile
- Ubicazione dei servizi e degli uffici CIE negli immobili
- Elenco del personale e sua assegnazione agli uffici.

Tali informazioni, in quanto considerate "sensibili", **devono essere trasmesse alla Prefettura in busta sigillata diversa da quella nella quale è contenuto il restante Piano di Sicurezza Comunale CIE**.

3.6.1. Ubicazione dei servizi e degli uffici CIE negli immobili

Per ogni ufficio elencato nella tabella "Allegato 3.2 Descrizione degli uffici e dei servizi", il Comune è tenuto a riportare l' immobile di riferimento e l'ubicazione degli uffici all'interno dell'immobile stesso.

Il Comune è quindi tenuto alla compilazione della seguente tabella.

Ufficio	Identificativo ufficio	Immobile	Ubicazione Immobile	Ubicazione dell'ufficio rispetto all'immobile

Compilare la tabella/modulo in conformità alle seguenti indicazioni:

- *Ufficio*: riportare la stessa classificazione degli uffici indicata al capitolo "3.3 Descrizione degli uffici". Qualora necessario per identificare univocamente l'ufficio, indicare anche il settore/area ed il servizio di riferimento.
- *Identificativo ufficio*: riportare l'identificativo dell'ufficio. Nel caso in cui un ufficio sia dislocato in più ambienti, è necessario assegnare un identificativo per ogni ambiente (ad esempio la numerazione della stanza).
- *Immobile*: riportare la denominazione dell'immobile (Palazzo Comunale, Circoscrizione, Municipio, od altro).
- *Ubicazione immobile*: Riportare l'indirizzo completo relativo all'immobile
- *Ubicazione dell'ufficio rispetto all'immobile*: riportare la descrizione dell'ubicazione dell'uffizio all'interno dell'immobile (per esempio piano terzo, stanza n. 4).

3.6.2. Descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza CIE

Per ciascun immobile di cui alla tabella del precedente paragrafo 3.6.1, è richiesta la descrizione dell'infrastruttura di sicurezza relativa ai seguenti aspetti:

- fisici e ambientali (per esempio inferriate di protezione per le finestre, porte blindate e altro ancora);
- organizzativi (sorveglianza, accesso ai locali, rapporti con altre istituzioni, e altro ancora);
- tecnologici (sistemi di allarme, sistemi di rilevazione incendi, e altro ancora).

In base alla classificazione precedente, per ogni immobile di interesse per la sicurezza CIE, il Comune è tenuto al corretto riempimento della seguente tabella.

Immobile		
Ubicazione		
Tipologia immobile		
Tipologia infrastruttura di sicurezza	Sistema di Sicurezza	Descrizione

Compilare la tabella/modulo in osservanza delle seguenti indicazioni:

- *Immobile*: riportare la denominazione dell'immobile (Palazzo Comunale, Delegazione o altro);
- *Ubicazione*: Riportare l'indirizzo completo relativo all'immobile;
- *Tipologia immobile*: descrivere la tipologia dell' immobile (per esempio appartamento, palazzo o altro ancora);

- *Tipologia infrastruttura di sicurezza*: riportare la tipologia dell'infrastruttura di sicurezza inserendo uno dei seguenti valori:
  - fisica e ambientali (per esempio inferriate di protezione per le finestre, porte blindate e altro ancora);
  - organizzativa (sorveglianza, accesso ai locali, rapporti con altre istituzioni, e altro ancora);
  - tecnologica (sistemi di allarme, sistemi di rilevazione incendi, e altro ancora).
- *Sistema di sicurezza*: riportare le caratteristiche strutturali del sistema di sicurezza (per esempio inferriate, sistema di allarme, sistema di sorveglianza e altro ancora);
- *Descrizione*: riportare breve descrizione sintetica delle caratteristiche tecniche del sistema di sicurezza.

3.6.3. Elenco del personale e sua assegnazione agli uffici

In base agli uffici descritti ed ai relativi ruoli previsti, il Comune è tenuto ad elencare il personale addetto indicando se personale a diretta dipendenza dell'amministrazione o se personale temporaneamente incaricato.

Il Comune è quindi tenuto al corretto riempimento della seguente tabella:

Ufficio	Ruolo	Nominativo del Personale	Personale temporaneamente incaricato (*)

(*) se il personale è temporaneamente incaricato, barrare la presente casella.

Compilare la tabella/modulo in osservanza delle seguenti indicazioni:

- *Ufficio*: riportare la stessa classificazione degli uffici effettuata al capitolo "3.3 Descrizione degli uffici". Qualora necessario per identificare univocamente l'ufficio, indicare anche il settore/area ed il servizio di riferimento.
- *Ruolo*: per l'ufficio di riferimento, riportare la stessa classificazione dei ruoli effettuata al capitolo "3.3 Descrizione degli uffici".
- *Nominativo del personale*: riportale il nominativo del personale che ricopre il ruolo di riferimento.
- *Personale temporaneamente incaricato*: se il personale è interno al comune, riportate il termine "interno" nella casella, se il personale è temporaneamente incaricato, barrare la casella con una ics.

Per ogni fornitore del Comune descrivere i servizi forniti al comune ed indicare la sede ed il responsabile di riferimento

Denominazione fornitore	Descrizione	Sede	Nominativo del responsabile di riferimento

Compilare la tabella/modulo secondo le seguenti indicazioni:

- *Denominazione fornitore*: riportare la denominazione dell'organismo
- *Descrizione*: riportare una descrizione sintetica dei servizi offerti dal fornitore
- *Sede*: riportare la sede del fornitore
- *Nominativo del responsabile di riferimento*: riportare il nominativo del responsabile del fornitore (per esempio chi ha firmato il contratto).

4. Macroprocessi e relativi flussi informativi di emissione ed uso CIE

4.1. Il macroprocesso di caricamento dell'INA

Il macroprocesso di caricamento dell'INA – Indice Nazionale delle Anagrafi, si articola nei seguenti processi:

- Acquisizione delle "*quantità di sicurezza, attivazione e certificazione*"
- Predisposizione della Porta di accesso ai domini applicativi del CNSD
- Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria - MEF
- Primo caricamento dell'Indice Nazionale delle Anagrafi
- Aggiornamento continuo dell'Indice Nazionale delle Anagrafi.

Nel seguito, per tutti i processi, si individua l'insieme di processi elementari che li compongono e dai quali sono stati estratti i singoli elementi (asset) oggetto del piano di sicurezza.

4.1.1. Acquisizione delle "*quantità di sicurezza, attivazione e certificazione*"

Le "*quantità di sicurezza, attivazione e certificazione*" costituiscono il supporto tecnologico-informatico necessario sia all'attivazione della porta di accesso ai domini applicativi del CNSD, sia alla registrazione, sulla porta di accesso, dei sistemi comunali che accedono ai domini applicativi del CNSD attraverso la porta di accesso stessa. Le "*quantità di sicurezza, attivazione e certificazione*" sono fornite dal Ministero dell'Interno e sono così composte:

- certificato digitale attribuito al responsabile comunale per la sicurezza degli accessi al CNSD
- strumenti software e di sicurezza (agenti di monitoraggio e controllo, certificati digitali per la registrazione dei sistemi comunali per utilizzare la porta di accesso, applicazioni software di servizio) richiesti per l'attivazione della Porta di accesso ai servizi applicativi del CNSD e per l'attivazione dei sistemi comunali autorizzati all'accesso ai servizi applicativi del CNSD.

Il Comune, richiede al Ministero dell'Interno l'acquisizione delle "*quantità di sicurezza, attivazione e certificazione*" e, una volta ricevute, le deposita presso un sito sicuro ed idoneo.

Le singole fasi sono le seguenti:
- Nomina del responsabile comunale per la sicurezza degli accessi al CNSD
- Richiesta delle "Quantità di sicurezza, attivazione e certificazione" al Ministero dell'Interno
- Ricezione dei certificati digitali per accedere al sito WEB del CNSD al fine di completare la richiesta delle "Quantità di sicurezza, attivazione e certificazione"
- Completamento della richiesta delle "Quantità di sicurezza, attivazione e certificazione"
- Ricezione delle "Quantità di sicurezza, attivazione e certificazione"
- Deposito delle "Quantità di sicurezza, attivazione e certificazione" presso una sede sicura del Comune, idonea al deposito di carte valori.

Il Comune deve immediatamente comunicare alla Prefettura ed al Ministero dell'Interno qualsiasi avvenimento che comprometta la sicurezza delle "quantità di sicurezza, attivazione e certificazione". La comunicazione deve avvenire seguendo le procedure previste per le comunicazioni formali.

I processi elementari sono i seguenti:

1) **Nomina del responsabile comunale per la sicurezza degli accessi al CNSD: il Sindaco nomina il responsabile comunale per la sicurezza degli accessi al CNSD. La nomina del responsabile comunale per la sicurezza degli accessi al CNSD deve essere comunicata dal Comune alla Prefettura ed al Ministero dell'Interno con le modalità indicate sul sito Internet del CNSD: processo elementare di back office**

   Controlli:
   - Deve essere prestata particolare attenzione
     - Al soddisfacimento di tutti i prerequisiti indicati dal Ministero dell'Interno e riportati sul sito del CNSD.

   Asset individuati:
   a. Informazioni
      i. Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD.
      ii. Direttive del Ministero dell'Interno.
   b. Reti
      i. -
   c. Infrastrutture
      i. Gli uffici comunali incaricati della custodia degli atti.
   d. Hardware
      i. -
   e. Software
      i. -
   f. Risorse umane
      i. Il Sindaco
      ii. Il responsabile comunale per la sicurezza degli accessi al CNSD.

2) Richiesta al Ministero dell'Interno delle "Quantità di sicurezza, attivazione e certificazione" e comunicazione ufficiale, al medesimo, del responsabile comunale per la sicurezza degli accessi al CNSD.

Controlli:
- Deve essere prestata particolare attenzione
  - Al soddisfacimento di tutti i prerequisiti indicati dal Ministero dell'Interno e riportati sul sito Internet del CNSD.

Asset individuati:

a. Informazioni
   i. Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD
   ii. Atto contenente la richiesta delle "Quantità di sicurezza, attivazione e certificazione".

b. Reti
   i. -.

c. Infrastrutture
   i. Gli uffici comunali incaricati della custodia degli atti.

d. Hardware
   i. -

e. Software
   i. -

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD
   iii. L'incaricato dell'invio al Ministero dell'Interno della richiesta delle "Quantità di sicurezza, attivazione e certificazione".

3) Ricezione dei certificati digitali per accedere allo specifico sito WEB del CNSD dedicato alla registrazione dei responsabili comunali per la sicurezza degli accessi al CNSD per completare la richiesta delle "Quantità di sicurezza, attivazione e certificazione"

Controlli:
- Deve essere prestata particolare attenzione
  - Alla gestione in sicurezza dei certificati digitali ricevuti.

Asset individuati:

a. Informazioni

i. Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD
ii. I certificati digitali per accedere al sito WEB del CNSD dedicato alla registrazione dei responsabili comunali per il completamento della richiesta delle "quantità di sicurezza, attivazione e certificazione".

b. Reti
   i. -.

c. Infrastrutture
   i. Gli uffici comunali incaricati della custodia degli atti.
   ii. Gli uffici comunali incaricati della custodia dei certificati digitali, predisposti dal Ministero dell'Interno, per l'accesso al sito WEB di registrazione, presso il CSND.

d. Hardware
   i. -

e. Software
   i. -

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD

4) Completamento della richiesta delle "Quantità di sicurezza, attivazione e certificazione"
Controlli:
- Deve essere prestata particolare attenzione
  - Alla gestione in sicurezza dei certificati digitali per l'accesso al sito WEB di registrazione, presso il CSND.

Asset individuati:

a. Informazioni
   i. Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD
   ii. I certificati digitali per accedere al sito WEB di registrazione presso il CNSD.

b. Reti
   i. Le reti comunali attraverso cui transitano i flussi informativi per il completamento della registrazione del responsabile comunale.

c. Infrastrutture
   i. Gli uffici comunali incaricati della custodia degli atti.
   ii. Gli uffici comunali incaricati della custodia dei certificati digitali per l'accesso al sito WEB di registrazione, presso il CSND.

d. Hardware
   i. -

e. Software
   i. -

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD.

5) Il Comune riceve dal Ministero dell'Interno le "Quantità di sicurezza, attivazione e certificazione" per cui ha fatto precedentemente richiesta: processo elementare di comunicazione.

Controlli:

- Deve essere prestata particolare attenzione
  - al trasporto delle "Quantità di sicurezza, attivazione e certificazione" alla sede di deposito,
  - alla verifica dell'integrità e del corretto funzionamento del supporto fisico su cui sono memorizzate le "Quantità di sicurezza, attivazione e certificazione"
  - alla verifica della precisa corrispondenza tra la denominazione del Comune destinatario, allegata alle "Quantità di sicurezza, attivazione e certificazione" ricevute, e la denominazione del Comune stesso,
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Atto di richiesta delle "Quantità di sicurezza, attivazione e certificazione".
   ii. Le "Quantità di sicurezza, attivazione e certificazione".
b. Reti
   i. Le reti di comunicazione del comune.
c. Infrastrutture
   i. Gli uffici comunali incaricati della presa in carico delle "Quantità di sicurezza, attivazione e certificazione" e dell'eventuale trasporto verso il luogo di custodia.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   i. Il responsabile comunale per la sicurezza degli accessi al CNSD
   ii. L'incaricato della presa in carico delle "Quantità di sicurezza, attivazione e certificazione".

6) Il Comune deposita le "Quantità di sicurezza, attivazione e certificazione" ricevute dal Ministero dell'Interno presso una sede idonea al deposito di carte valori: processo elementare di Back office.

Controlli:

- Deve essere prestata particolare attenzione
  - alle procedure di deposito che devono registrare in modo preciso chi ha effettuato la consegna e quando la stessa è stata effettuata,
  - alla verifica di conformità del sito in cui sono depositate la "Quantità di sicurezza, attivazione e certificazione" rispetto alle norme relative al deposito delle carte valori,
  - alle modalità di registrazione degli accessi a tale deposito, in particolare modo nel caso in cui siano depositati nello stesso luogo altri beni o altre carte valori.

Asset individuati:

a. Informazioni
   i. Gli atti che indicano chi è responsabile della gestione dell'ufficio in cui sono depositate le "Quantità di sicurezza, attivazione e certificazione".
   ii. Le "Quantità di sicurezza, attivazione e certificazione".
b. Reti
   i. Le reti comunali coinvolte nei flussi informativi connessi al processo di deposito delle "Quantità di sicurezza, attivazione e certificazione".
c. Infrastrutture
   i. Gli uffici comunali incaricati della presa in carico delle "Quantità di sicurezza, attivazione e certificazione" e dell'eventuale trasporto al deposito.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD
   iii. L'incaricato della presa in carico delle "Quantità di sicurezza, attivazione e certificazione".
   iv. L'incaricato del deposito delle "Quantità di sicurezza, attivazione e certificazione".

4.1.2. Predisposizione Porta di Accesso ai Domini applicativi del CNSD

Il Comune, al fine di accedere ai servizi offerti dai domini applicativi del CNSD, deve predisporre ed attivare la Porta di accesso ai domini applicativi del CNSD.

I Comuni accedono a tutti i servizi erogati in rete dal CNSD, esclusivamente attraverso la propria porta di accesso ai domini applicativi del CNSD, attivata ed abilitata per l'accesso agli specifici servizi.
La porta di accesso ai domini applicativi del CNSD costituisce, quindi, il punto di presa in carico di tutte le comunicazioni provenienti dal Comune (flussi di emissione della CIE, aggiornamenti INA, interrogazioni/aggiornamenti AIRE, altri servizi anagrafici) e del loro successivo inoltro al CNSD. Tale porta di accesso certifica il punto di origine delle comunicazioni, individuando univocamente il Comune che comunica con il CNSD: **tutte le comunicazioni devono quindi avvenire esclusivamente tramite la porta di accesso del Comune ai domini applicativi del CNSD**.

Tutte le comunicazioni di rete relative alle richieste di servizio, transitano per la porta di accesso che verifica le quantità di sicurezza utilizzate dal Comune per tali comunicazioni tramite Backbone, inserisce le richieste di servizio in un'apposita busta informatica creata dalla Porta stessa secondo le specifiche del Sistema Pubblico di Connettività (busta di e-gov) e le invia ai sistemi centrali Backbone del CNSD.

Le comunicazioni tra i sistemi comunali e la porta di accesso avvengono secondo il protocollo XML SOAP o Post HTTP XML e devono essere identificate e rese sicure attraverso l'uso delle quantità di sicurezza fornite dal Ministero dell'Interno ai Comuni. Il sistema degli agenti di monitoraggio e allarmi, attivi sulla Porta di Accesso dei Comuni, segnala al CNSD tutte le anomalie (sicurezza, qualità e livelli di servizio) riscontrate nelle fasi di trasmissione dei flussi applicativi e nel funzionamento delle reti comunali.
Presso il CNSD tutte le richieste di servizio provenienti dai Comuni attraverso le porte di accesso, transitano per i sistemi centrali Backbone che verificano la corretta trasmissione delle buste di e-gov e la corrispondenza tra le richieste di servizio pervenute ed i servizi effettivamente registrati presso i sistemi centrali Backbone. In caso positivo, le richieste di servizio sono riportate ai corrispondenti domini applicativi del CNSD per essere trattate e per la formulazione delle relative risposte.

Le singole fasi sono le seguenti:
1) Installazione e prima configurazione dell'hardware e del software di base della porta di accesso
2) configurazione dell'infrastruttura di rete comunale
3) installazione della porta tramite le "quantità di sicurezza, attivazione e certificazione", attivazione Backbone del CNSD, attivazione agenti di monitoraggio ed allarmi.
4) Verifica di funzionamento e collegamento in rete della porta di accesso ai domini applicativi del CNSD e, in caso positivo, attivazione della porta stessa.

Al completamente positivo della fase 4 la porta di accesso ai domini applicativi del CNSD si considera operativa e certificata nel funzionamento.

I processi elementari sono i seguenti:

1) **Installazione e prima configurazione dell'hardware e del software di base della porta di accesso del Comune, in base alle regole tecniche indicate dal Ministero dell'Interno: processo elementare di back office.**

Controlli:

- Deve essere prestata particolare attenzione
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Indicazioni sulle caratteristiche del software di base della porta di accesso, fornite dal Ministero dell'Interno
   ii. Archivio delle abilitazioni per l'uso dei sistemi comunali
b. Reti
   i. -
c. Infrastrutture
   i. La sede ove il Comune installa la Porta di accesso ai domini applicativi del CNSD.
d. Hardware
   i. I sistemi hardware utilizzati per la Porta di accesso ai domini applicativi del CNSD.
e. Software
   i. Il software di base della Porta di accesso ai domini applicativi del CNSD.
f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD

2) **Configurazione dell'infrastruttura di rete comunale: attività di back office per la configurazione delle sezioni di rete comunale necessarie alle comunicazioni tra la porta di accesso ed il CNSD.**

Controlli:

- Deve essere prestata particolare attenzione
  - alle indicazioni Ministero sulla configurazione della rete comunale,
  - alla gestione della sicurezza nei segmenti di rete comunale coinvolti,
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Direttive ed indicazioni del Ministero dell'Interno.
   ii. Archivio delle abilitazioni per l'uso dei sistemi comunali.
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
   ii. La rete dati del Comune per le comunicazioni verso il CNSD.

c. Infrastrutture
    i. La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati.
d. Hardware
    i. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD.
e. Software
    i. -.
f. Risorse umane
    i. Il responsabile dei sistemi informatici del Comune
    ii. Il responsabile dei sistemi di rete del Comune
    iii. Il responsabile comunale per la sicurezza degli accessi al CNSD.

3) Installazione della porta di accesso ai domini del CNSD, utilizzando le "quantità di sicurezza, attivazione e certificazione", attivazione Backbone CNSD, attivazione degli agenti di monitoraggio ed allarmi: processo elementare di back office.

Controlli:
- Deve essere prestata particolare attenzione
    - alla gestione dei supporti fisici contenenti le "quantità di sicurezza, attivazione e certificazione",
    - alla configurazione del software di base dell'elaboratore che ospita i software della Porta di accesso ai domini applicativi del CNSD,

Asset individuati:
a. Informazioni
    i. Archivio delle abilitazioni per l'uso dei sistemi comunali,
    ii. "quantità di sicurezza, attivazione e certificazione" e software della Porta di accesso ai domini applicativi del CNSD, predisposti dal Ministero dell'Interno.
b. Reti
    i. Le reti di comunicazione dati del Comune per le comunicazioni verso la porta di accesso e, attraverso questa, verso il CNSD,
c. Infrastrutture
    i. La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati.
    ii. La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".
    iii. Gli uffici eventualmente incaricati del trasporto delle "Quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede in cui è stata installata la Porta di accesso ai domini applicativi del CNSD.
d. Hardware

i. I supporti su cui sono memorizzate le “quantità di sicurezza, attivazione e certificazione” ed il software della Porta di accesso ai domini applicativi del CNSD.
   ii. Il computer (pc, server, …) su cui installare il software della Porta di accesso ai domini applicativi del CNSD.
   iii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD.

e. Software
   i. Il software della Porta di accesso ai domini applicativi del CNSD,
   ii. gli agenti software di monitoraggio ed allarme.

f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dei sistemi di rete del Comune
   iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
   iv. I tecnici che devono installare la Porta di accesso ai domini applicativi del CNSD.
   v. Il call center del CNSD che supporta e verifica la corretta installazione della Porta di accesso ai domini applicativi del CNSD.

4) Verifica di funzionamento e collegamento in rete della porta di accesso ai domini applicativi del CNSD e, in caso positivo, attivazione della porta stessa: processo elementare di back office.

Controlli:

- Deve essere prestata particolare attenzione
  - alla gestione delle “Quantità di sicurezza, attivazione e certificazione”,
  - alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
  - alla gestione della sicurezza delle reti comunali coinvolte.

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l’uso dei sistemi comunali
   ii. “Quantità di sicurezza, attivazione e certificazione”.

b. Reti
   i. La rete dati del Comune per le comunicazioni verso il CNSD.

c. Infrastrutture
   i. La sede presso cui il Comune conserva le “quantità di sicurezza, attivazione e certificazione”.
   ii. Gli uffici eventualmente incaricati del trasporto delle “quantità di sicurezza, attivazione e certificazione” dalla sede di deposito alla sede in cui è installata la porta di accesso ai domini applicativi del CNSD.

iii. La sede/i presso cui il Comune ha installato la porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati.

d. Hardware
   i. Il computer (pc, server, …) su cui è stata installato il software della porta di accesso ai domini applicativi del CNSD.
   ii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD.
e. Software
   i. Il software della porta di accesso ai domini applicativi del CNSD e le relative applicazioni software di supporto.
f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dei sistemi di rete del Comune
   iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
   iv. L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".
   v. Il Call center del CNSD che fornisce supporto all'esecuzione delle verifiche di funzionamento e connessione in rete per l'attivazione operativa della Porta di accesso ai domini applicativi del CNSD.

4.1.3. Predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi INA del CNSD

Ai fini dell'accesso ai domini applicativi del CNSD, i sistemi comunali devono inviare le loro richieste di servizio alla porta di accesso comunale.
Per ridurre i rischi negli scambi informativi in rete tra i sistemi comunali e la porta di accesso, è stata prevista una procedura di attivazione dei sistemi comunali sulla porta di accesso.
La procedura di attivazione di un sistema comunale sulla porta di accesso, per l'accesso ai servizi applicativi INA del CNSD richiede:

1. Registrazione del sistema comunale sulla porta di accesso ai domini applicativi del CNSD
2. Verifica della corretta configurazione delle comunicazioni tra i sistemi comunali e la porta di accesso per l'accesso ai servizi del CNSD

I processi elementari sono i seguenti:

1) **Registrazione del sistema comunale sulla porta di accesso ai domini applicativi del CNSD: processo elementare di back office**

   Controlli:
   - Deve essere prestata particolare attenzione
     - alla gestione delle "Quantità di sicurezza, attivazione e certificazione" utilizzate per registrare il sistema comunale sulla porta di accesso ai domini applicativi del CNSD

- alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD;
- alla definizione dei diritti di accesso ai sistemi comunali che si devono registrare alla Porta di accesso ai domini applicativi del CNSD;
- alla gestione della sicurezza delle reti comunali coinvolte

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l'uso dei sistemi comunali
   ii. "Quantità di sicurezza, attivazione e certificazione".

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.

c. Infrastrutture
   i. La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".
   ii. Gli uffici eventualmente incaricati del trasporto della "quantità di sicurezza, attivazione e certificazione"dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD.
   iii. La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati
   iv. Le sedi in cui sono installati i sistemi comunali che devono essere messi in comunicazione con la porta di accesso

d. Hardware
   i. Il computer (pc, server, …) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.
   ii. L'hardware dei sistemi comunali da collegare alla porta di accesso
   iii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.

e. Software
   i. L'applicativo software per la registrazione e l'attivazione di comunicazioni in rete crittografate in base a certificati digitali, contenuto nelle "quantità di sicurezza, attivazione e certificazione, ed installato sui sistemi comunali che devono essere collegati alla porta di accesso.

f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dei sistemi di rete del Comune
   iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
   iv. L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".
   v. Il Call center del CNSD che fornisce supporto ai Comuni per la registrazione dei sistemi comunali alla Porta di accesso ai domini applicativi del CNSD.

2) Verifica della corretta configurazione delle comunicazioni tra i sistemi comunali e la porta di accesso ai domini applicativi del CNSD: processo elementare di back office

Controlli:

- Deve essere prestata particolare attenzione
  - alla gestione della "Quantità di sicurezza, attivazione e certificazione",
  - alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
  - alla definizione dei diritti di accesso ai sistemi comunali che devono comunicare con la porta di accesso,
  - alla gestione della sicurezza delle reti comunali coinvolte

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l'uso dei sistemi comunali
   ii. "Quantità di sicurezza, attivazione e certificazione".
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
   ii. La rete dati del Comune per le comunicazioni verso il CNSD.
c. Infrastrutture
   i. La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".
   ii. Gli uffici eventualmente incaricati del trasporto della "quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD.
   iii. La sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD
   iv. Le sedi in cui sono installati i sistemi comunali che devono essere messi in comunicazione con la porta di accesso
d. Hardware
   i. Il computer (pc, server, …) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.
   ii. L'hardware dei sistemi comunali da collegare alla porta di accesso
   iii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.
e. Software
   i. L'applicativo software per la verifica delle comunicazioni certificate tra i sistemi comunali e la porta di accesso

f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dei sistemi di rete del Comune
   iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
   iv. L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".
   v. Il Call center del CNSD che fornisce supporto nelle verifiche della sussistenza e completezza delle comunicazioni tra i sistemi comunali e la

Porta di accesso ai domini applicativi del CNSD e tra quest'ultima ed il CNSD.

4.1.4. Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria

Il Comune deve allineare i Codici Fiscali presenti presso la propria anagrafe (sia essa in formato cartaceo che elettronico) con i relativi archivi dell'Anagrafe Tributaria del MEF (Ministero di Economia e Finanze).

Le singole fasi sono le seguenti:

1) **Il Comune estrae dalla propria anagrafe le corrispondenze tra dati anagrafici e codici fiscali, ivi compresi i dati anagrafici ai quali non è associato un codice fiscale: processo elementare di elaborazione.**

   CONTROLLI:
   - Deve essere prestata particolare attenzione
     - alla gestione delle copie di sicurezza dell'anagrafe locale
     - all'estrazione dei dati anagrafici,
     - alla gestione del dispositivo fisico di memorizzazione dell'archivio delle corrispondenze,
     - alla sicurezza delle reti coinvolte.
     - alla continuità del servizio in caso di incidenti e eventi straordinari
     - alla gestione degli accessi alle risorse

   Asset individuati:
   a. Informazioni
      i. Archivio anagrafico del Comune;
      ii. Archivio delle corrispondenze dato anagrafico⇔codice fiscale: output del processo.
      iii. Archivio delle abilitazioni per l'uso dei sistemi comunali: input del processo.
   b. Reti
      i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
   c. Infrastrutture
      i. La/e sede/i comunale/i dell'archivio anagrafico comunale.
      ii. La/e sede/i comunale/i presso cui l'archivio delle corrispondenze viene depositato.
      iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze.
   d. Hardware
      i. Il/i sistema/i comunale/i di gestione ed archiviazione dei dati anagrafici.
      ii. Il/i terminale/i da cui si accede all'anagrafe per attivare la procedura di estrazione dell'archivio delle corrispondenze.
      iii. I dispositivi di memorizzazione dell'archivio delle corrispondenze.

iv. La porta di accesso ai domini applicativi del CNSD

e. Software
   i. Il Sistema Informativo Comunale
   ii. I servizi di estrazione dei dati anagrafici dall'archivio anagrafico comunale.
   iii. Il software d'estrazione delle corrispondenze.
   iv. Il Software di memorizzazione dell'archivio delle corrispondenze sui dispositivi hardware preposti.

f. Risorse umane
   i. Il responsabile dell'anagrafe
   ii. Il responsabile del Sistema Informativo Comunale
   iii. I tecnici informatici incaricati dell'attuazione del processo di estrazione e creazione dell'archivio delle corrispondenze.
   iv. L'incaricato del deposito dell'archivio delle corrispondenze

2) Il Comune, a partire dalle corrispondenze così ottenute, predispone un archivio utilizzando le specifiche definite dall'Anagrafe Tributaria: processo elementare di elaborazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
   - alle copie di sicurezza dei dati informativi
   - alla conversione dell'archivio nel formato richiesto da anagrafe tributaria,
   - alla gestione dei supporti fisici su cui tali archivi sono memorizzati,
   - alla sicurezza delle reti coinvolte.
   - alla continuità del servizio anche in caso di incidenti o eventi straordinari
   - alla gestione degli accessi alle risorse

Asset individuati:

a. Informazioni.
   i. Archivio delle corrispondenze dato anagrafico⇔codice fiscale: input del processo.
   ii. Archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria: output del processo.
   iii. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati

c. Infrastrutture
   i. La/e sede/i comunale/i presso cui è presente l'archivio delle corrispondenze.
   ii. La/e sede/i comunale/i presso cui l'archivio predisposto per l'Anagrafe Tributaria viene depositato.
   iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze.

d. Hardware

i. Il/i terminale/i da cui si accede all'anagrafe per attivare la procedura di strutturazione dell'archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria.
ii. I dispositivi di memorizzazione dell'archivio delle corrispondenze.
iii. I dispositivi di memorizzazione dell'archivio predisposto nel formato richiesto dall'Anagrafe Tributaria.

e. Software
i. Il software di trasformazione dell'archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria.
ii. Il Software di memorizzazione dell'archivio delle corrispondenze nel formato archivio richiesto da Anagrafe Tributaria sui dispositivi hardware preposti.

f. Risorse umane
i. I tecnici informatici incaricati dell'attuazione del processo di trasformazione dell'archivio delle corrispondenze.
ii. Gli incaricati del deposito dell'archivio delle corrispondenze e dell'archivio trasformato nel formato richiesto da Anagrafe Tributaria.

3) Il Comune invia l'archivio così formato all'Anagrafe Tributaria: processo elementare di comunicazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei supporti fisici su cui l'archivio è memorizzato,
  - alla gestione della sicurezza delle reti coinvolte.
  - alle copie di sicurezza dei dati informativi
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari
  - alla gestione degli accessi alle risorse

Asset individuati:

a. Informazioni.
i. Archivio delle corrispondenze nel formato richiesto da Anagrafe Tributaria: input del processo.
ii. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
iii. Archivio delle "ricevute" fornite da Anagrafe Tributaria come conferma della ricezione dell'archivio delle corrispondenze anagrafe-codici fiscali.

b. Reti
i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
ii. La rete verso il CNSD e Anagrafe Tributaria.

c. Infrastrutture
i. La/e sede/i comunale/i presso cui l'archivio predisposto per Anagrafe Tributaria viene depositato.
ii. La sede/i da cui il Comune trasmette i dati verso Anagrafe Tributaria.

iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze da consegnare ad Anagrafe Tributaria.

d. Hardware
   i. Il/i terminale/i da cui si accede per inviare l'archivio delle corrispondenze in rete.
   ii. La Porta di accesso ai domini applicativi del CNSD per l'accesso al Backbone del CNSD, utilizzato per la certificazione e la sicurezza della trasmissione dell'archivio delle corrispondenze e delle relative ricevute da parte di Anagrafe Tributaria.
   iii. I dispositivi di memorizzazione dell'archivio delle corrispondenze.
   iv. I dispositivi di memorizzazione dell'archivio delle "ricevute" di Anagrafe Tributaria.

e. Software
   i. Il software di invio dell'archivio delle corrispondenze verso Anagrafe Tributaria e di ricezione delle ricevute, attraverso la Porta di accesso ai domini applicativi del CNSD ovvero direttamente ad Anagrafe Tributaria.
   ii. Il Software di archiviazione delle ricevute di Anagrafe Tributaria.

f. Risorse umane
   i. I tecnici informatici incaricati dell'attuazione del processo di invio dell'archivio delle corrispondenze e della ricezione delle "ricevute" di Anagrafe Tributaria.
   ii. Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze e dell'archivio delle ricevute di Anagrafe Tributaria.

4) L'Anagrafe Tributaria verifica la coerenza dell'archivio, attribuisce o aggiorna i codici fiscali non presenti o non allineati, segnala le corrispondenze non assegnate. L'Anagrafe Tributaria invia al Comune l'archivio di corrispondenze aggiornato: processo elementare di comunicazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei supporti fisici su cui l'archivio è memorizzato,
  - alla gestione dei diritti di ricezione dell'archivio allineato da parte di anagrafe tributaria,
  - alla gestione della sicurezza delle reti coinvolte.
  - alle copie di sicurezza dei dati informativi
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari
  - alla gestione degli accessi alle risorse

Asset individuati:

a. Informazioni.
   i. Archivio delle corrispondenze aggiornato da Anagrafe Tributaria: input del processo.
   ii. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.

iii. Archivio delle “ricevute” fornite da Anagrafe Tributaria come conferma della ricezione dell’archivio delle corrispondenze anagrafe-codici fiscali.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
   ii. La rete verso il CNSD e l’Anagrafe Tributaria.

c. Infrastrutture
   i. La sede/i da cui il Comune riceve i dati allineati da anagrafe tributaria.
   ii. La/e sede/i comunale/i presso cui l’archivio allineato da Anagrafe Tributaria viene depositato.

d. Hardware
   i. Il/i terminale/i da cui si accede per ricevere l’archivio delle corrispondenze allineato da anagrafe tributaria.
   ii. La Porta di accesso ai domini applicativi del CNSD per l’accesso al Backbone del CNSD, utilizzato per la certificazione e la sicurezza della ricezione dell’archivio delle corrispondenze allineate.
   iii. I dispositivi di memorizzazione dell’archivio delle corrispondenze allineate.
   iv. I dispositivi di memorizzazione dell’archivio delle “ricevute” di Anagrafe Tributaria.

e. Software
   i. Il software di ricezione dell’archivio delle corrispondenze allineate da anagrafe tributaria attraverso la porta di dominio comunale.
   ii. Il Software di accesso alle ricevute di anagrafe tributaria.
   iii. Il software di verifica della corrispondenza tra le ricevute di presa in consegna da parte di anagrafe tributaria degli archivi di corrispondenze non allineati con gli archivi delle corrispondenze allineate ricevuti da anagrafe tributaria.

f. Risorse umane
   i. I tecnici informatici incaricati dell’attuazione del processo di ricezione dell’archivio delle corrispondenze e verifica con le “ricevute” di anagrafe tributaria.
   ii. Lo/gli incaricato/i del deposito dell’archivio delle corrispondenze allineate e dell’archivio delle ricevute di Anagrafe Tributaria.

5) Il Comune, per ogni elemento dell’archivio di corrispondenze, aggiorna nella propria anagrafe le corrispondenze tra dato anagrafico e codice fiscale: processo elementare di elaborazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei diritti di accesso alla procedura di aggiornamento dell’anagrafe,
  - alla gestione della sicurezza delle reti coinvolte.
  - alle copie di sicurezza dei dati informativi
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari
  - alla gestione degli accessi alle risorse

Asset individuati:

a. Informazioni.
   i. Archivio anagrafico del Comune.
   ii. Archivio delle corrispondenze aggiornato da Anagrafe Tributaria e verificato con l'archivio delle ricevute di anagrafe tributaria: input del processo.
   iii. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
c. Infrastrutture
   i. La sede/i da cui il Comune elabora le corrispondenze allineati da anagrafe tributaria
   ii. La/e sede/i comunale/i presso cui l'archivio delle corrispondenze allineate da Anagrafe Tributaria è stato depositato.
d. Hardware
   i. Il Sistema Informativo Comunale
   ii. Il/i terminale/i da cui si accede per attivare la procedura di inserimento delle corrispondenze allineate nell'anagrafe comunale.
   iii. I dispositivi di memorizzazione dell'archivio delle corrispondenze allineate.
e. Software
   i. Il software di riallineamento dell'anagrafe comunale a partire dall'archivio delle corrispondenze allineato da anagrafe tributaria
f. Risorse umane
   i. Il responsabile del Sistema Informativo Comunale
   ii. Il responsabile dell'anagrafe
   iii. I tecnici informatici incaricati dell'attuazione del processo di riallineamento
   iv. Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze allineate.

6) Il Comune, per tutti i casi di non corrispondenza, inizia una serie di attività di recupero dei codici fiscali per le corrispondenze non assegnate dall'Anagrafe Tributaria: processo elementare di elaborazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei supporti fisici su cui l'archivio delle mancate corrispondenze è memorizzato,
  - alla definizione dei diritti di trattamento di questa tipologia di dati,
  - alla gestione della sicurezza delle reti coinvolte,
  - alle copie di sicurezza dei dati informativi,
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari,
  - alla gestione degli accessi alle risorse.

Si noti come questa fase possa, per tutte le corrispondenze non allineate per le quali il Comune ritiene di aver individuato una soluzione, confluire nella fase precedente di invio all'Anagrafe Tributaria di un nuovo archivio per l'allineamento delle corrispondenze.

Asset individuati:

a. Informazioni.
   i. Archivio anagrafico del Comune.
   ii. Archivio dei dati anagrafici non ancora allineati.
   iii. Archivio delle abilitazioni per l'uso dei sistemi comunali.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati

c. Infrastrutture
   i. La sede/i presso cui il Comune elabora le corrispondenze non allineate da anagrafe tributaria
   ii. La/e sede/i comunale/i presso cui l'archivio delle corrispondenze non allineate dall'Anagrafe Tributaria è stato depositato.

d. Hardware
   i. Il Sistema Informativo Comunale
   ii. Il/i terminale/i da cui si accede per attivare la procedura di correzione delle corrispondenze non allineate nell'anagrafe comunale.
   iii. I dispositivi di memorizzazione dell'archivio delle corrispondenze non allineate.

e. Software
   i. Il software per la creazione e la gestione dell'archivio delle corrispondenze "dato anagrafico – codice fiscale" non ancora allineate.

f. Risorse umane
   i. Il responsabile dei Sistemi Informatici del Comune
   ii. Il responsabile dell'anagrafe
   iii. I tecnici informatici incaricati dell'attuazione del processo di riallineamento
   iv. Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze non ancora allineate.

4.1.5. Primo caricamento dell'Indice Nazionale delle Anagrafi.

Il Comune predispone un estratto della propria anagrafe contenente i soli dati anagrafici di cui è stato verificato l'allineamento con i codici fiscali dell'anagrafe tributaria, nel formato richiesto per il primo caricamento dell'INA e lo invia al CNSD.

1) **Predisposizione dell'archivio anagrafico nel formato previsto per il primo caricamento dell'Indice Nazionale delle Anagrafi, da inviare, attraverso la Porta di accesso ai domini applicativi del CNSD, al CNSD: processo elementare di elaborazione.**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei supporti fisici su cui l'archivio per il primo caricamento INA è memorizzato,

- alla definizione dei diritti di accesso alla procedura di estrazione dei dati dall'anagrafe comunale,
- alla gestione della sicurezza delle reti comunali coinvolte
- alle copie di sicurezza dei dati informativi,
- alla continuità del servizio anche in caso di incidenti o eventi straordinari,
- alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Archivio anagrafico del Comune
   ii. Archivio delle abilitazioni per l'uso dei sistemi comunali .
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
c. Infrastrutture
   i. Il Sistema Informativo Comunale
   ii. La sede presso cui il Comune archivia l'archivio anagrafico per il primo caricamento dell'INA.
   iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviati i dati di primo caricamento dell'INA dalla sede in cui sono stati estratti, alla sede in cui devono essere temporaneamente archiviati o alla sede destinata al successivo invio dei dati.
d. Hardware
   i. Il Sistema Informativo Comunale
   ii. Il terminale da cui è attivata la procedura di estrazione dei dati dall'anagrafe nel formato richiesto per il primo caricamento dell'INA.
e. Software
   i. La procedura software per la strutturazione dei dati anagrafici nel formato richiesto dal primo caricamento dell'INA.
f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dell'anagrafe
   iii. Lo/gli incaricato/i dell'archiviazione dell'archivio anagrafico da inviare successivamente all'INA.
   iv. L'operatore che attiva la procedura di formazione dell'archivio di primo caricamento dell'INA.

2) **Invio al CNSD dei dati anagrafici per il primo caricamento dell'INA: processo elementare di comunicazione. Il Comune, attraverso la Porta di accesso ai domini applicativi del CNSD, si connette al CNSD, servizio di primo caricamento dell'INA, e gli invia i dati anagrafici acquisendo la ricevuta di invio effettuato.**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei trasferimenti (in rete o su supporto fisico) dei dati del primo caricamento INA,

- alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
- alla gestione della sicurezza delle reti comunali coinvolte
- alle copie di sicurezza dei dati informativi,
- alla continuità del servizio anche in caso di incidenti o eventi straordinari,
- alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
   ii. Archivio di primo caricamento dell'INA
   iii. Ricevuta dell'invio effettuato.
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
   ii. La rete dati del Comune per le comunicazioni verso il CNSD.
c. Infrastrutture
   i. La sede/i presso cui il Comune ha archiviato l'archivio di primo caricamento dell'INA.
   ii. La sede del Comune presso cui è installata la Porta di accesso ai domini applicativi del CNSD.
   iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato il primo caricamento dell'INA dalla sede di archiviazione alla sede di invio al CNSD.
d. Hardware
   i. La Porta di accesso ai domini applicativi del CNSD.
   ii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.
e. Software
   i. La Porta di accesso ai domini applicativi del CNSD.
   ii. Il software di invio al CNSD dell'archivio del primo caricamento dell'INA.
f. Risorse umane
   i. Il responsabile delle reti
   ii. Il responsabile della Porta di accesso ai domini applicativi del CNSD
   iii. Lo/gli incaricato/i del trattamento dell'archivio relativo al primo caricamento dell'INA.
   iv. Lo/gli incaricato/i dell'archiviazione delle ricevute, fornite dal CNSD, dell'invio effettuato,
   v. L'operatore incaricato dell'invio al CNSD del primo caricamento dell'INA e dell'acquisizione della ricevuta di invio effettuato.
   vi. Il Call center del CNSD a supporto delle operazioni di invio al CNSD.

4.1.6. Aggiornamento continuo dell'Indice Nazionale delle Anagrafi.

Il Comune, attraverso un insieme di procedure automatizzate o manuali, invia in tempo reale o a cadenze prefissate, non superiori alle 24 ore, tutte le variazioni anagrafiche intervenute presso l'anagrafe comunale, al CNSD per l'aggiornamento dell'INA. L'invio è effettuato utilizzando il modello WEB, inviando un file XML dai sistemi comunali alla Porta di accesso ai domini applicativi del CNSD, secondo una delle seguenti modalità:

- Post XML su protocollo http
- Protocollo XML SOAP secondo le specifiche del Sistema Pubblico di Connettività (Busta SPCoop, estensione standard di SOAP 1.1)

La Porta di accesso ai servizi applicativi del CNSD, verifica la conformità dei flussi informativi, predispone la "busta e-gov" secondo le specifiche del Sistema Pubblico di Connettività (Busta SPCoop, estensione standard di SOAP 1.1) ed invia la stessa al CNSD gestendo tutte le credenziali di sicurezza relative all'infrastruttura Backbone.

Tutti i comuni che già utilizzano il software applicativo PCCSA, potranno continuare ad utilizzare tale software fino al 31/12/2005, ovvero fino alla scadenza del periodo transitorio previsto per il passaggio alla modalità di comunicazione precedentemente indicata. In seguito si farà riferimento sia al software applicativo PCCSA relativo alla gestione del transitorio, sia al modello WEB di invio del file XML.

1) **Acquisizione ed installazione del software di supporto all'invio delle variazioni anagrafiche al CNSD: processo elementare di comunicazione.**
   Il Comune riceve dal Ministero dell'Interno – CNSD, il software di supporto all'invio delle variazioni anagrafiche secondo i formati XML o XML SOAP.

   CONTROLLI:
   - Deve essere prestata particolare attenzione
     - alla gestione dei trasferimenti (in rete o su supporto fisico) del software di invio,
     - alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
     - alla gestione della sicurezza delle reti comunali coinvolte
     - alla continuità del servizio anche in caso di incidenti o eventi straordinari,
     - alla gestione degli accessi alle risorse.

   Asset individuati:
   a. Informazioni
      i. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
   b. Reti
      i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
      ii. La rete dati del Comune per le comunicazioni verso il CNSD.
   c. Infrastrutture

i. La sede/i presso cui il Comune archivia il software di invio delle variazioni anagrafiche ricevuto dal Ministero dell'Interno.
   ii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato il software di invio delle variazioni anagrafiche (nel caso in cui il software sia fornito attraverso gli uffici del Ministero dell'Interno e, quindi, ci sia un trasporto fisico dei supporti (cdrom, dvd,nastro, …).

d. Hardware
   i. Il terminale utilizzato per connettersi al CNSD per richiedere e acquisire il software di invio delle variazioni anagrafiche.
   ii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.

e. Software
   i. Il software di supporto all'invio delle variazioni anagrafiche nei formati XML o XML SOAP.

f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile delle reti
   iii. Il responsabile della Porta di accesso ai domini applicativi del CNSD
   iv. Lo/gli incaricato/i di archiviare il software ricevuto dal Ministero dell'Interno.

2) Predisposizione dell'archivio contenente le variazioni anagrafiche da inviare al CNSD per l'aggiornamento dell'INA: processo elementare di elaborazione. I formati sono, per i comuni che ancora utilizzano il software PCCSA, il formato accettato da PCCSA, oppure il formato XML di strutturazione delle variazioni anagrafiche.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei trasferimenti (in rete o su supporto fisico) dei dati di aggiornamento dell'INA,
  - alla definizione dei diritti di accesso alla procedura che consente di estrarre tali dati dall'anagrafe comunale,
  - alla gestione della sicurezza delle reti comunali coinvolte,
  - alle copie di sicurezza dei dati informativi,
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari,
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
   ii. Archivio anagrafico.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.

c. Infrastrutture
   i. La sede/i dell'archivio anagrafico
   ii. La sede del Comune presso cui depositare temporaneamente l'archivio di aggiornamento dell'INA.
   iii. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici tra le sedi coinvolte.
d. Hardware
   i. I sistemi informatici del Comune
e. Software
   i. Il Sistema Informativo Comunale
   ii. La procedura software di estrazione e strutturazione in uno dei formati richiesti, degli aggiornamento anagrafici da inviare al CNSD.
f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dell'anagrafe
   iii. Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA.
   iv. L'operatore incaricato dell'attivazione della procedura di formazione dell'archivio di aggiornamento dell'INA da inviare al CNSD.
   v. Il Call center del CNSD a supporto dei comuni.

3) Invio al CNSD dell'archivio delle variazioni anagrafiche per l'aggiornamento dell'INA: processo elementare di comunicazione. Il Comune, attraverso la Porta di accesso ai domini applicativi del CNSD, si connette al CNSD, servizio di aggiornamento dell'INA, ed invia l'archivio. L'invio può essere realizzato attraverso l'attivazione (manuale o automatica) del software PCCSA fino al 31/12/2005 per i Comuni che intendano ancora utilizzare tale modalità. Dal 1/1/2006, l'unica modalità di invio accettata, è rappresentata dall'invio delle variazioni anagrafiche in formato XML o XML SOAP. Il Comune acquisisce una ricevuta di invio effettuato.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione dei trasferimenti (in rete o su supporto fisico) dei dati di aggiornamento dell'INA,
  - alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
  - alla gestione, per i comuni che lo utilizzano, dei diritti di accesso al software PCCSA,
  - alla gestione della sicurezza delle reti comunali coinvolte,
  - alle copie di sicurezza dei dati informativi,
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari,
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni

i. Archivio delle abilitazioni per l'uso dei sistemi comunali : input del processo.
ii. Archivio di aggiornamento dell'INA
iii. Ricevuta, fornita dal CNSD, dell'invio effettuato.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
   ii. La rete dati del Comune per le comunicazioni verso il CNSD.
c. Infrastrutture
   i. La sede/i presso cui il Comune ha depositato l'archivio di aggiornamento dell'INA.
   ii. La sede da cui il Comune effettua l'invio dell'aggiornamento INA al CNSD attraverso la porta di accesso
   iii. La sede del Comune presso cui è installata la Porta di accesso ai domini applicativi del CNSD.
   iv. Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato l'aggiornamento dell'INA dalla sede di archiviazione alla sede di invio al CNSD.
d. Hardware
   i. La Porta di accesso ai domini applicativi del CNSD.
   ii. i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.
e. Software
   i. La Porta di accesso ai domini applicativi del CNSD.
   ii. Il software per l'invio al CNSD, attraverso la Porta di accesso ai domini applicativi dello stesso, dell'aggiornamento dell'INA oppure, fino al 31/12/2005, il software PCCSA.
f. Risorse umane
   i. Il responsabile delle reti
   ii. Il responsabile della Porta di accesso ai domini applicativi del CNSD
   iii. Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA.
   iv. Lo/gli incaricato/i dell'archiviazione delle ricevute, fornite dal CNSD, dell'invio effettuato,
   v. L'operatore incaricato dell'invio al CNSD dell'aggiornamento dell'INA e dell'acquisizione della ricevuta di invio effettuato.
   vi. Il Call center del CNSD a supporto dei Comuni.

4.2. Il macroprocesso di emissione CIE

Il macroprocesso di emissione della CIE, si articola nei seguenti processi e sottoprocessi elementari:

- Nomina del responsabile della CIE
- Predisposizione delle Postazioni di Emissione
- Attivazione delle Postazioni di Emissione ai servizi applicativi di emissione CIE del CNSD

- Acquisizione della quantità di sicurezza
- Acquisizione delle CIE inizializzate dall'Istituto Poligrafico
- Rilascio delle CIE ai cittadini

Si evidenzia che il Macroprocesso di caricamento dell'INA è propedeutico al macroprocesso di emissione CIE.

Nel seguito, per ogni processo, si individua l'insieme di attività e flussi informativi elementari che li compongono e dai quali è possibile estrarre, quindi, i singoli elementi (asset) oggetto del piano di sicurezza.

4.2.1. Nomina del responsabile della sicurezza CIE

Il Sindaco nomina il responsabile comunale della sicurezza CIE denominato anche responsabile CIE. La nomina del responsabile della Sicurezza CIE del Comune, deve essere comunicata nelle modalità indicate dal Ministero dell'Interno sul sito web del CNSD (www.servizidemografici.interno.it)

CONTROLLI:

- Deve essere prestata particolare attenzione
  - Al soddisfacimento di tutti i pre-requisiti e requisiti richiesti dal Ministero dell'Interno

Asset individuati:

a. Informazioni
   i. Atti di nomina del responsabile della CIE.
   ii. Direttive del Ministero dell'Interno
b. Reti
   i. -.
c. Infrastrutture
   i. Le strutture organizzative adibite alla custodia degli atti.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile comunale per la sicurezza degli accessi al CNSD
   iii. Il responsabile della CIE

4.2.2. Predisposizione delle Postazioni di Emissione

Il Comune installa la/le postazioni di emissione e tutte le altre componenti hardware necessarie all'emissione CIE, presso le sedi comunali individuate per il rilascio e la formazione (stampa) della CIE ai cittadini.

Le singole fasi sono le seguenti:

1) **Il Comune installa presso le sedi designate le postazioni di emissione: processo elementare di elaborazione. Le postazioni di emissione sia di front office che di back office devono essere installate su un segmento di rete che consenta la comunicazione tra postazione/i di emissione e la Porta di accesso ai domini applicativi del CNSD e da questa verso il CNSD.**

   CONTROLLI:
   - Deve essere prestata particolare attenzione
     - alla gestione delle installazioni (hardware e, più in particolare, software) degli apparati presso le sedi designate dal Comune,
     - alla definizione dei diritti di accesso a tali apparati, ivi compresa la configurazione di software antivirus,
     - al blocco delle configurazioni dei dispositivi collegati agli apparati sia direttamente (lettori, stampanti…), sia attraverso la rete (firewall…),
     - alla gestione della sicurezza delle reti comunali che consentono a tali apparati di colloquiare tra loro, di comunicare con la Porta di accesso ai domini applicativi del CNSD e, attraverso quest'ultima, di comunicare con il SSCE
     - alla continuità del servizio anche in caso di incidenti o eventi straordinari,
     - alla gestione degli accessi alle risorse.

   Asset individuati:
   a. Informazioni
      i. -.
   b. Reti
      i. Le reti dati del Comune alle quali collegare le postazioni di emissione.
      ii. La rete presso cui è installata la Porta di accesso ai domini applicativi del CNSD di accesso al backbone del CNSD.
      iii. La rete che consente alle postazioni di emissione di comunicare tra loro, di comunicare con la Porta di accesso ai domini applicativi del CNSD e, attraverso questo, di comunicare con il SSCE.
      iv. La protezione fisica dei dispositivi di rete attraverso cui passano le comunicazioni delle postazioni di emissione verso la Porta di accesso ai domini applicativi del CNSD e da questa verso il CNSD.
   c. Infrastrutture
      i. Gli uffici comunali ove sono installate le postazioni di emissione.
   d. Hardware
      i. La protezione fisica delle postazioni di emissione e della Porta di accesso ai domini applicativi del CNSD e di tutti gli apparati (lettore/scrittore di chip,

stampante termica e relativo lettore di chip, lettore/scrittore di banda laser,…) ad esse connesse.

e. Software
   i. -.
f. Risorse umane
   i. Il responsabile della CIE
   ii. Gli operatori ed i tecnici incaricati di installare gli apparati di emissione e di configurare il relativo software di base.
   iii. Il call center CIE

4.2.3. Attivazione delle Postazioni di Emissione ai servizi applicativi di emissione CIE del CNSD

La porta di accesso ai domini applicativi del CNSD è l'unico punto comunale di accesso ai servizi applicativi del CNSD. Tutti i sistemi comunali che devono accedere ai servizi applicativi del CNSD devono essere registrati alla Porta di accesso ai domini applicativi del CNSD.
Il Comune richiede al Ministero dell'Interno l'abilitazione all'installazione dei software di supporto al rilascio della CIE ai cittadini, di comunicazione con i servizi centrali di gestione delle sospensioni, revoche o riattivazioni delle CIE.

La procedura di attivazione delle postazioni di emissione per l'accesso ai servizi applicativi di emissione CIE del CNSD richiede:

1) **Abilitazione del sistema all'accesso del servizio applicativo del CNSD tramite "quantità di sicurezza, attivazione e certificazione": processo elementare di back office per l'attivazione degli agenti di monitoraggio ed allarmi**

   CONTROLLI:
   - Deve essere prestata particolare attenzione
     - alla gestione dei supporti fisici su cui sono memorizzate le "quantità di sicurezza, attivazione e certificazione",
     - alla gestione della sicurezza delle reti comunali coinvolte.
     - alla continuità del servizio anche in caso di incidenti o eventi straordinari
     - alla gestione degli accessi alle risorse

   Asset individuati:
   a. Informazioni
      i. Archivio delle abilitazioni per l'uso dei sistemi comunali
      ii. "quantità di sicurezza, attivazione e certificazione".
   b. Reti
      i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
      ii. La rete dati del Comune per le comunicazioni verso il CNSD.
   c. Infrastrutture
      i. La sede/i comunale che ospita/no le postazioni di emissione.

ii. Le strutture operative eventualmente incaricate del trasporto delle "Quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede/i in cui sono state installate le postazioni di emissione.
iii. La/e sede/i presso cui sono installate le postazioni di emissione

d. Hardware
  i. Hardware delle postazioni di emissione.
  ii. I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni relative all'emissione di CIE.

e. Software
  i. Il software di emissione CIE
  ii. Il Software degli agenti di monitoraggio ed allarmi.

f. Risorse umane
  i. Il responsabile dei sistemi informatici del Comune
  ii. Il responsabile delle reti
  iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
  iv. Il responsabile della CIE,
  v. I tecnici che gestiscono i sistemi comunali,
  vi. L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione",
  vii. Il call center del CNSD che supporta i tecnici comunali nell'attivazione degli agenti di monitoraggio ed allarmi

2) Verifica della corretta configurazione dei canali di comunicazione: processo elementare di back office

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alla gestione delle "Quantità di sicurezza, attivazione e certificazione",
  - alla definizione dei diritti di accesso alla Porta di accesso ai domini applicativi del CNSD,
  - alla definizione dei diritti di accesso alle postazioni di emissione,
  - alla gestione della sicurezza delle reti comunali coinvolte
  - alla gestione degli accessi alle risorse

Asset individuati:

a. Informazioni
  i. Archivio delle abilitazioni per l'uso dei sistemi comunali
  ii. "Quantità di sicurezza, attivazione e certificazione".

b. Reti
  i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
  ii. La rete dati del Comune per le comunicazioni verso il CNSD.

c. Infrastrutture

i. La sede presso cui il Comune deposita le “quantità di sicurezza, attivazione e certificazione”.
   ii. Le strutture operative eventualmente incaricate del trasporto della “quantità di sicurezza, attivazione e certificazione” dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD.
   iii. La sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD
   iv. La/e sede/i presso cui sono installate le postazioni di emissione

d. Hardware
   i. Il computer (pc, server, …) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.
   ii. Hardware delle postazioni di emissione
   iii. I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.

e. Software
   i. Gli strumenti software per le verifiche di connettività, disponibili tra le “quantità di sicurezza, attivazione e certificazione”.

f. Risorse umane
   i. Il responsabile dei sistemi informatici comunali
   ii. Il responsabile dei sistemi di rete comunali
   iii. Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD
   iv. Il responsabile della CIE
   v. Lo/gli incaricato/i del deposito delle “quantità di sicurezza, attivazione e certificazione”.
   vi. Il Call center del CNSD che fornisce supporto per la corretta esecuzione delle verifiche di comunicazione.

4.2.4. Acquisizione delle quantità di sicurezza

Le “quantità di sicurezza” costituiscono il supporto tecnologico-informatico di archiviazione fornito dal Ministero e contenente le credenziali richieste per la comunicazione con i servizi di emissione CIE.

Il Comune, richiede al Ministero dell’Interno le Quantità di Sicurezza e, quindi, l’abilitazione all’emissione delle CIE. Le riceve e le deposita presso un sito sicuro ed idoneo.
Le singole fasi sono le seguenti:
- Richiesta delle Quantità di Sicurezza al Ministero dell’Interno
- Ricezione delle Quantità di Sicurezza, con modalità di trasporto carte valori
- Deposito delle Quantità di Sicurezza presso una sede sicura del Comune, idonea al deposito di carte valori.

Le singole fasi sono le seguenti:

1) Richiesta delle Quantità di Sicurezza al Ministero dell'Interno

CONTROLLI:

- Deve essere prestata particolare attenzione
  - o alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   iii. Richiesta delle Quantità di Sicurezza.
   iv. Gli atti di nomina del responsabile dell'invio delle richieste al Ministero dell'Interno.
   v. Direttive del Ministero dell'Interno
b. Reti
   i. Le reti comunali coinvolte nei flussi informativi connessi all'effettuazione della richiesta.
c. Infrastrutture
   i. -.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile della CIE
   iii. Lo/gli incaricato/i dell'effettuazione della richiesta.
   iv. Il call center CIE

2) Il Comune riceve dal Ministero dell'Interno le Quantità di Sicurezza per cui ha fatto precedentemente richiesta: processo elementare di comunicazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - o al vettore utilizzato per il trasporto delle Quantità di Sicurezza alla sede di deposito,
  - o alla verifica dell'integrità e del corretto funzionamento del supporto di memorizzazione della quantità di sicurezza
  - o alla verifica della corrispondenza tra quantità di sicurezza ricevute e denominazione del Comune,
  - o alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Richiesta delle Quantità di Sicurezza.

ii. Gli atti di nomina del responsabile della presa in carico della quantità di sicurezza.
iii. Atti relativi alla presa in carico delle quantità di sicurezza

b. Reti
   i. -.
c. Infrastrutture
   i. Le strutture organizzative adibite alla presa in carico della quantità di sicurezza ed all'eventuale trasporto verso il luogo di custodia.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   v. Il responsabile della CIE
   vi. Lo/gli incaricato/i della presa in carico della quantità di sicurezza.
   vii. Il call center CIE

3) Il Comune deposita le quantità di sicurezza ricevute dal Ministero dell'Interno presso una sede idonea al deposito di carte valori: processo elementare di Back office.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - al vettore utilizzato per portare le quantità di sicurezza alla sede di deposito,
  - alle procedure di deposito che devono registrare in modo preciso l'avvenuta consegna e il relativo vettore,
  - alla verifica di rispondenza del sito in cui è depositata le quantità di sicurezza rispetto alle norme sul deposito delle carte valori,
  - alle modalità di registrazione di chiunque abbia accesso a tale deposito, in particolar modo nel caso in cui siano depositate nello stesso luogo altri beni o altre carte valori,
  - alla continuità del servizio anche in caso di incidenti o eventi straordinari.

Asset individuati:

a. Informazioni
   i. Le Quantità di Sicurezza.
   ii. Gli atti di nomina dei responsabili del deposito e della gestione dei relativi locali.
b. Reti
   i. -.
c. Infrastrutture
   i. Le strutture organizzative adibite alla presa in carico delle quantità di sicurezza presso il deposito ed all'eventuale trasporto al deposito stesso.
d. Hardware
   i. -

e. Software
    i. -
f. Risorse umane
    i. Il Sindaco
    ii. Il responsabile della CIE
    iii. Lo/gli incaricato/i della presa in carico della quantità di sicurezza.
    iv. Lo/gli incaricato/i del deposito della quantità di sicurezza.
    v. Il call center CIE.

4.2.5. Acquisizione delle CIE inizializzate

Il Comune, richiede al Ministero dell'Interno l'invio di un lotto di CIE da rilasciare ai cittadini, lo riceve e lo deposita presso un sito sicuro ed idoneo.
Le singole fasi sono le seguenti:

- Richiesta di un lotto di CIE al Ministero dell'Interno
- Ricezione di un lotto di CIE, con le modalità di trasporto delle carte valori
- Deposito delle CIE inizializzate presso una sede sicura del Comune, idonea al deposito di carte valori.

Le singole fasi sono le seguenti:

1) **Il Comune richiede un lotto di CIE al Ministero dell'Interno: processo elementare di comunicazione.**

CONTROLLI:

- Deve essere prestata particolare attenzione
    - alla gestione delle quantità richieste al fine di verificare, all'arrivo delle CIE, la corrispondenza precisa tra CIE richieste e CIE ricevute
    - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
    i. Il numero di CIE richieste.
    ii. Gli atti di nomina del responsabile dell'invio delle richieste al Ministero dell'Interno.
b. Reti
    i. -
c. Infrastrutture
    i. -.
d. Hardware
    i. -
e. Software
    i. -
f. Risorse umane
    i. Il Sindaco
    ii. Il responsabile della CIE

iii. Lo/gli incaricato/i dell'effettuazione della richiesta di CIE.
iv. Il call center CIE

2) Il Comune riceve dalla Prefettura un lotto di CIE, di cui ha fatto precedentemente richiesta: processo elementare di comunicazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - al vettore utilizzato per portare le CIE alla sede di deposito, una volta ricevute le CIE dalla Prefettura,
  - alla verifica della corrispondenza tra il numero di CIE ricevute e il nunero di CIE richieste,
  - alla verifica di rispondenza della personalizzazione delle CIE, fatta dall'Istituto Poligrafico e Zecca dello Stato, con il Comune stesso[1].
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Il numero di CIE richieste.
   ii. Gli atti di nomina del responsabile della presa in carico delle CIE.
b. Reti
   i. -.
c. Infrastrutture
   i. Le strutture organizzative adibite alla presa in carico delle CIE ed all'eventuale trasporto verso la sede idonea alla loro conservazione.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile della CIE
   iii. Lo/gli incaricato/i della presa in carico delle CIE.
   iv. Il call center CIE

3) Il Comune deposita le CIE ricevute dalla Prefettura presso una sede idonea al deposito di carte valori: processo elementare di elaborazione.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - al vettore utilizzato per portare le CIE alla sede di deposito,

---

[1] Si ricorda che le CIE sono "personalizzate" sul comune, nel senso che una CIE, quando viene fornita ad un Comune, è stata inizializzata dall'Istituto Poligrafico e Zecca dello Stato con informazioni che ne rendono impossibile l'utilizzo da parte di un altro Comune.

- alle procedure di deposito che devono registrare in modo preciso l'avvenuta consegna e il relativo vettore,
- alla verifica di rispondenza del sito in cui sono depositate le CIE rispetto alle norme sul deposito delle carte valori,
- alle modalità di registrazione di chiunque abbia accesso a tale deposito, nel caso in cui siano depositate nello stesso luogo altri beni o altre carte valori,
- alla continuità del servizio anche in caso di incidenti o eventi straordinari.

Asset individuati:

a. Informazioni
   i. Il numero di CIE depositate.
   ii. Gli atti di nomina dei responsabili del deposito delle CIE e della gestione del sito in cui sono depositate le CIE.

b. Reti
   i. -.

c. Infrastrutture
   i. Le strutture organizzative adibite alla presa in carico delle CIE presso il deposito ed all'eventuale trasporto al deposito stesso.

d. Hardware
   i. -

e. Software
   i. -

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile della CIE
   iii. Lo/gli incaricato/i della presa in carico delle CIE.
   iv. Lo/gli incaricato/i del deposito delle CIE.
   v. Il call center CIE.

4.2.6. Rilascio CIE ai cittadini

Il Comune attiva gli sportelli di rilascio della CIE ai cittadini. Definisce lo/gli incaricato/i reposti all'utilizzo dei vari apparati di emissione e stampa della CIE, definisce gli orari di accesso al pubblico ed inizia a rilasciare CIE ai suoi cittadini.
Il modello di riferimento per l'emissione delle CIE è costituito dal modello asincrono di emissione.

Le fasi di rilascio sono le seguenti:

Fase 1. Acquisizione quantità di sicurezza per il punto di Back office di collegamento ai servizi di emissione CIE
Fase 2. Approvvigionamento CIE inizializzate dall'Istituto Poligrafico per il punto di back office di allestimento CIE
Fase 3. Acquisizione dei dati dai cittadini
Fase 4. Invio della richiesta di emissione ad SSCE

Fase 5. Ricezione, dai servizi di emissione CIE, degli elementi necessari al rilascio
Fase 6. Lavorazione elettronica e grafica delle CIE
Fase 7. Attivazione CIE e rilascio ai cittadini
Fase 8. Riconsegna CIE
Fase 9. Riconsegna quantità di sicurezza

1) **Acquisizione quantità di sicurezza per il punto di Back office di collegamento ai servizi di emissione CIE: processo elementare di elaborazione. Lo/gli incaricato/i del punto di back office di collegamento ai servizi CIE richiede allo/agli incaricato/i il prelievo della quantità di sicurezza dal deposito (idoneo alle carte valori).**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alle procedure di identificazione e autorizzazione di coloro che sono coinvolti nel processo,
  - alla redazione dei rapporti di consegna e restituzione,
  - alle fasi di trasporto dal deposito al punto di backoffice.
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Quantità di sicurezza
   ii. I rapporti di consegna (e presa in carico).
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
c. Infrastrutture
   i. La sede di deposito delle quantità di sicurezza
   ii. Le strutture utilizzate per il trasporto delle quantità di sicurezza tra le due sedi.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile CIE.
   iii. Lo/gli incaricato/i del deposito e del prelievo e consegna delle quantità di sicurezza.

2) **Approvvigionamento CIE inizializzate dall'Istituto Poligrafico per il punto di back office di allestimento CIE: processo elementare di elaborazione. Lo/gli incaricato/i del rilascio CIE da un punto di back office di allestimento della CIE richiede allo/agli incaricato/i del prelievo delle CIE dal deposito (idoneo alle carte valori), di prelevare un lotto di CIE da deposito e di consegnarglielo.**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alle procedure di identificazione e autorizzazione di coloro che sono coinvolti nel processo,
  - alla redazione dei rapporti di consegna CIE,
  - alle fasi di trasporto CIE dal deposito al punto di back office di allestimento CIE.
  - alla gestione degli accessi alle risorse.

Asset individuati:

a. Informazioni
   i. Le CIE richieste
   ii. I rapporti di consegna (e presa in carico) delle CIE.
b. Reti
   i. -.
c. Infrastrutture
   i. La sede di deposito delle CIE
   ii. La sede di rilascio delle CIE ai cittadini.
   iii. Le strutture utilizzate per il trasporto delle CIE tra le due sedi.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile CIE.
   iii. Lo/gli incaricato/i del deposito e del rilascio CIE.

3) **Acquisizione dei dati dai cittadini: processo elementare di Front Office. Il cittadino fornisce i suoi dati anagrafici e biometrici (acquisiti con i dispositivi di lettura impronta). Il Comune, attraverso il collegamento della postazione di Front office con l'anagrafe comunale, esegue una prima verifica dei dati del cittadino, prelevando dall'anagrafe tutte le informazioni utili all'emissione della CIE. I dati anagrafici e biometrici così ottenuti sono inviati alla postazione di back office per l'allestimento delle CIE.**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - all'attribuzione dei privilegi di accesso ai punti di emissione di front office per l'acquisizione dei dati (password, smart card, token card, lettore di impronta, …),
  - alle procedure di identificazione dei cittadini,
  - alle procedure di acquisizione dei dati biometrici ed anagrafici dei cittadini,
  - all'accesso ai locali dove sono acquisite le informazioni anagrafiche e biometriche dei cittadini che hanno richiesto il rilascio della CIE,

- alla gestione della sicurezza delle reti comunali coinvolte, particolarmente per quei tratti di rete in cui transitano le comunicazioni anagrafiche tra l'anagrafe e il punto di front office di acquisizione dati.

Asset individuati:

a. Informazioni
   i. Archivio anagrafico del Comune.
   ii. Archivio delle abilitazioni per l'accesso ai dati anagrafici.
   iii. I dati anagrafici e biometrici dei cittadini.

b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.

c. Infrastrutture
   i. Il Sistema Informativo Comunale
   ii. La sede presso cui si acquisiscono i dati anagrafici dei cittadini.

d. Hardware
   i. I sistemi informatici del Comune
   ii. il punto di front office di acquisizione dei dati ed i relativi apparati per l'acquisizione dei dati anagrafici e biometrici dei cittadini.
   iii. Il punto di Back office per l'allestimento delle CIE.

e. Software
   i. La procedura software di acquisizione dei dati anagrafici e biometrici installata sulla postazione di front office di acquisizione dati.
   ii. La procedura software per l'integrazione con l'anagrafe comunale, installata sulla postazione di front office di acquisizione dati,.

f. Risorse umane
   i. Il responsabile dei sistemi informatici del Comune
   ii. Il responsabile dell'anagrafe
   iii. Il responsabile della CIE
   iv. L'operatore incaricato del rilascio CIE.

4) Invio della richiesta di emissione ad SSCE: processo elementare di comunicazione di back office. Lo/gli incaricato/i del punto di back office per l'allestimento della CIE che gestisce le comunicazione con SSCE, invia la/e richiesta/e di emissione ai servizi di emissione CIE. I servizi di emissione CIE forniscono una ricevuta dell'avvenuto invio.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - all'attribuzione dei privilegi di accesso al punto di back office per l'allestimento della CIE(username/password, smart card, token card, lettore di impronta, …), al punto di back office per il collegamento ai servizi di emissione CIE attraverso la Porta di accesso ai domini applicativi del CNSD,
  - all'accesso ai locali dove è presente il punto di back office di allestimento delle CIE, il punto di back soffice per la comunicazione con i servizi di emissione CIE e il punto di accesso ai domini applicativi del CNSD ,
  - al trattamento delle ricevute di invio effettuato,

- o alla gestione della sicurezza delle reti comunali coinvolte, particolarmente per quei tratti di rete in cui transitano le comunicazioni tra:
    - punto di back office di allestimento CIE
    - punto di back office per la comunicazione con i servizi di emissione CIE
    - Porta di accesso ai domini applicativi del CNSD.

Asset individuati:

a. Informazioni
   i. Richiesta di emissione
   ii. Ricevuta della richiesta di emissione
   iii. Archivio delle abilitazioni per l'uso dei sistemi comunali.
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati .
c. Infrastrutture
   i. La/e sede/i presso cui sono installate le postazioni di back office di allestimento della CIE
   ii. La sede presso cui è installata la postazione di back office per la comunicazione ai servizi di emissione CIE
   iii. La sede presso cui è presente la Porta di accesso ai domini applicativi del CNSD
d. Hardware
   i. Hardware delle postazioni di back office di allestimento della CIE.
   ii. Hardware delle postazioni di back office per la comunicazione ai servizi di emissione CIE.
   iii. Hardware della Porta di accesso ai domini applicativi del CNSD.
e. Software
   i. La procedura software di invio delle richieste ad SSCE, presente sulle postazioni di back office di allestimento della CIE.
   ii. La procedura software presente sulla postazione di back office di comunicazione con i servizi SSCE.
f. Risorse umane
   i. Il responsabile della CIE
   ii. Lo/gli incaricato/i dell'invio delle richieste di emissione CIE tramite una postazione di emissione.

5) Ricezione, dai servizi di emissione CIE, degli elementi necessari al rilascio: processo elementare di comunicazione di back office. Lo/gli incaricato/i del punto di back office di allestimento della CIE, riceve le autorizzazioni (certificati, …) per il rilascio della/e CIE.

CONTROLLI:

- Deve essere prestata particolare attenzione

- all'attribuzione dei privilegi di accesso al punto di back office per l'allestimento delle CIE, al punto di back office per la comunicazione con i servizi di emissione CIE, alla porta di accesso ai domini applicativi del CNSD (username/password, smart card, token card, lettore di impronta, …),
- all'accesso ai locali dove è presente il punto di back office per l'allestimento delle CIE, il punto di back office per la comunicazione con i servizi di emissione CIE, la porta di accesso ai domini applicativi del CNSD,
- alla gestione dei dati ricevuti da SSCE, attraverso la porta di accesso ai domini del CNSD, di autorizzazione al rilascio CIE,
- alla gestione della sicurezza delle reti comunali coinvolte, particolarmente per quei tratti di rete in cui transitano le comunicazioni tra:.
  - punto di back office di allestimento CIE
  - punto di back office per la comunicazione con i servizi di emissione CIE
  - Porta di accesso ai domini applicativi del CNSD

Asset individuati:

a. Informazioni
   i. Autorizzazione all'emissione
   ii. Archivio delle abilitazioni per l'uso dei sistemi comunali.
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
c. Infrastrutture
   i. La sede presso cui è presente il punto di back office di allestimento della CIE
   ii. La sede presso cui è presente il punto di back office per la comunicazione ai servizi di emissione CIE
   iii. La sede presso cui è presente la Porta di accesso ai domini applicativi del CNSD
d. Hardware
   i. Hardware delle postazioni di back office di allestimento della CIE.
   ii. Hardware della postazione di back office per la comunicazione ai servizi di emissione CIE.
   iii. Hardware della Porta di accesso ai domini applicativi del CNSD.
e. Software
   i. La procedura software di invio delle richieste ad SSCE, presente sul punto di back office di allestimento della CIE.
   ii. La procedura software presente sul punto di back office di comunicazione con i servizi SSCE.
f. Risorse umane
   i. Il responsabile della CIE
   ii. L'operatore incaricato della ricezione delle autorizzazioni all'emissione CIE.

6) **Lavorazione elettronica e grafica delle CIE: processo elementare di elaborazione. Lo/gli incaricato/i del punto di back office di allestimento della CIE che gestisce la lavorazione elettronica e grafica della CIE (stampa, scrittura sulla banda laser, scrittura sul microchip, …) a partire dalle autorizzazioni (certificati, …) per il rilascio della/e CIE ricevute da SSCE ed a partire dai dati anagrafici e biometrici dei**

cittadini, precedentemente acquisiti dal punto di front office di acquisizione dei dati, provvede alla lavorazione elettronica e grafica dei supporti (CIE).
CONTROLLI:

- Deve essere prestata particolare attenzione
  - all'attribuzione dei privilegi di accesso al punto di back office di allestimento della CIE (username/password, smart card, token card, lettore di impronta, …) dedicata a tale lavorazione,
  - al corretto accoppiamento tra dati anagrafici e biometrici dei cittadini e dati autorizzativi al rilascio della CIE,
  - alle corrette configurazioni dei dispositivi ed apparati utilizzati per la lavorazione grafica ed elettronica delle CIE al fine di garantire in ogni caso la correttezza della corrispondenza tra i dati memorizzati nel certificato digitale ed i dati stampati sulla CIE,
  - all'accesso ai locali dove è presente il punto di back office di allestimento della CIE che esegue la lavorazione elettronica e grafica della CIE,
  - alla gestione dei dati ricevuti da SSCE di autorizzazione al rilascio CIE,
  - alla gestione dei report (chi, dove, cosa, come e quando) sulle lavorazioni non andate a buon fine,
  - alla gestione e presa in carico delle CIE la cui lavorazione non è andata a buon fine,
  - alla gestione della sicurezza delle reti comunali coinvolte.

Asset individuati:

a. Informazioni
   i. Autorizzazioni all'emissione
   ii. Dati anagrafici e biometrici dei cittadini
   iii. Archivio delle abilitazioni per l'uso dei sistemi comunali.
   iv. CIE stampate correttamente
   v. CIE non stampate correttamente
   vi. Report sulle operazioni di stampa concluse correttamente
   vii. Report sulle operazioni di stampa non concluse correttamente
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
c. Infrastrutture
   i. La sede presso cui è presente la postazione di back office per l'allestimento delle CIE che esegue la lavorazione elettronica e grafica delle CIE.
d. Hardware
   i. Hardware della postazione di back office per l'allestimento delle CIE che esegue la lavorazione elettronica e grafica delle CIE.
e. Software
   i. La procedura software che gestisce la lavorazione elettronica e grafica delle CIE, presente sulla postazione di back office per l'allestimento delle CIE.
f. Risorse umane
   i. Il responsabile della CIE
   ii. L'operatore incaricato della lavorazione elettronica e grafica delle CIE.

7) Attivazione CIE e rilascio ai cittadini: processo elementare di front office. Lo/gli incaricato/i del punto di front office per il rilascio della CIE, punto che gestisce l'attivazione CIE e rilascio ai cittadini, prende in consegna le CIE stampate correttamente, identifica i cittadini per i quali la CIE è stata predisposta (anche attraverso connessione in rete a servizi comunali e/o nazionali di supporto all'identificazione), attiva la CIE e la rilascia la stessa al cittadino.

CONTROLLI:

- Deve essere prestata particolare attenzione
  - all'attribuzione dei privilegi di accesso al punto di front office per il rilascio della CIE (username/password, smart card, token card, lettore di impronta, …),
  - all'accesso ai locali dove è presente il punto di front office per il rilascio della CIE,
  - alla gestione dei lotti di CIE la cui stampa è andata a buon fine e che quindi possono essere attivati e consegnati ai cittadini,
  - alla gestione dei report (chi, dove, cosa, come e quando) sulle consegne non effettuate,
  - alla gestione e presa in carico delle CIE non consegnate,
  - alla gestione della sicurezza delle reti comunali coinvolte.

Asset individuati:

a. Informazioni
   i. Archivio delle abilitazioni per l'uso dei sistemi comunali.
   ii. CIE stampate correttamente
   iii. Report sulle operazioni di attivazione e consegna CIE concluse regolarmente
   iv. Report sulle operazioni di attivazione e consegna CIE non concluse regolarmente.
   v. Dati anagrafici dei cittadini per la loro identificazione in fase di consegna delle CIE personalizzate
b. Reti
   i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati
   ii. Le reti dati del Comune verso la porta di accesso ai servizi del CNSD e, attraverso questa, ai servizi di convalida anagrafica del CNSD, ai servizi di verifica validità del certificato CIE del SSCE, ai servizi di attivazione CIE del SSCE
c. Infrastrutture
   i. Le sedi presso cui sono presenti i punti di front office di rilascio e attivazione della CIE
d. Hardware
   i. Hardware delle postazioni di front office di rilascio e attivazione CIE.
e. Software
   i. La procedura software che gestisce l'attivazione delle CIE, presente sul punto di front office di rilascio e attivazione CIE.

f. Risorse umane
   i. Il responsabile della CIE
   ii. Lo/gli incaricato/i dell'attivazione e consegna delle CIE ai cittadini.

8) **Riconsegna CIE a deposito: processo elementare di comunicazione. Lo/gli incaricato/i della riconsegna delle CIE riporta le CIE non utilizzate allo/agli incaricato/i del deposito delle CIE (idoneo alle carte valori).**

CONTROLLI:
- Deve essere prestata particolare attenzione
  - alle procedure di identificazione e autorizzazione di coloro che sono coinvolti nel processo,
  - alla redazione dei rapporti di riconsegna CIE (ricordare che la differenza tra il numero di CIE prelevate con quelle riconsegnate in quanto non utilizzate, andate in errore o non rilasciate al cittadino per sua indisponibilità, deve essere zero),
  - alle fasi di trasporto delle CIE riconsegnate dal punto di back office di allestimento della CIE al deposito,
  - al deposito ed ai report delle CIE andate in errore o non consegnate a causa della mancata disponibilità di un cittadino.

Asset individuati:

a. Informazioni
   i. Le CIE non utilizzate
   ii. Le CIE non stampate correttamente
   iii. Le CIE non consegnate per indisponibilità del cittadino
   iv. I rapporti di consegna (e presa in carico) delle CIE
   v. Gli atti ed i documenti di autorizzazione al deposito o alla consegna CIE

b. Reti
   i. -.

c. Infrastrutture
   i. La sede deposito delle CIE
   ii. La/e sede/i di rilascio delle CIE ai cittadini.

d. Hardware
   i. -

e. Software
   i. -

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile CIE.
   iii. Lo/gli incaricato/i del deposito e della riconsegna CIE.

9) **Riconsegna quantità di sicurezza: processo elementare di comunicazione back office. Lo/gli incaricato/i riporta la quantità di sicurezza allo/agli incaricato/i incaricato del deposito della quantità di sicurezza (idoneo alle carte valori).**

CONTROLLI:

- Deve essere prestata particolare attenzione
  - alle procedure di identificazione e autorizzazione di coloro che sono coinvolti nel processo,
  - alla redazione dei rapporti di riconsegna della Quantità di Sicurezza,
  - alle fasi di trasporto della quantità di sicurezza dal punto di back office per la comunicazione con i servizi di emissione CIE al deposito,

Asset individuati:

a. Informazioni
   i. Le quantità di sicurezza
   ii. I relativi rapporti di consegna (e presa in carico)
   iii. Gli atti ed i documenti di autorizzazione al deposito o alla consegna delle quantità di sicurezza
b. Reti
   i. -.
c. Infrastrutture
   i. La sede deposito delle quantità di sicurezza
   ii. La sede del punto di back office per la comunicazione con i servizi di emissione CIE.
   iii. -.
d. Hardware
   i. -
e. Software
   i. -
f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile CIE.
   iii. Lo/gli incaricato/i del deposito e della riconsegna delle quantità di sicurezza.

4.3. Il macroprocesso di uso della CIE

Il macroprocesso di uso della CIE, attiene all'suo della CIE da parte di un cittadino (cui è stata rilasciata la CIE da un Comune) che accede, in rete, ad un servizio comunale. Il macroprocesso si articola nei seguenti processi e sottoprocessi elementari:

- Abilitazione di una postazione di lavoro al riconoscimento in rete della CIE
- Abilitazione di un server comunale per l'identificazione in rete dei cittadini tramite CIE.

Nel seguito, per ogni processo, si individua l'insieme di attività e flussi informativi elementari che li compongono e dai quali è possibile estrarre, quindi, i singoli elementi (asset) oggetto del piano di sicurezza.

4.3.1. Abilitazione di una postazione di lavoro al riconoscimento in rete dei cittadini che accedono tramite CIE ai servizi comunali

Si illustrano di seguito le fasi che devono essere svolte per consentire ad una postazione di lavoro di accettare la CIE come strumento di identificazione in rete di un cittadino.

Sulla postazione di lavoro che deve essere abilitata all'identificazione in rete utilizzando carte CIE, devono essere installati, in sicurezza, i software di verifica del certificato di sicurezza CIE, forniti dal Ministero dell'Interno.
Taòli software consentono l'accesso ai sistemi distribuiti per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE.

CONTROLLI:
- Deve essere prestata particolare attenzione:
  - Al fatto che, ai fini del riconoscimento in rete del cittadino attraverso la CIE, è sufficiente il solo certificato di sicurezza presente sulla CIE e non è quindi necessario che i dati anagrafici del cittadino siano inviati in rete.
    È infatti possibile per i WEB server autorizzati, nell'ambito dei servizi distribuiti del CNSD per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche, richiedere direttamente al Ministero dell'Interno i dati anagrafici sintetici associati ad un particolare certificato digitale CIE.
  - Alla sicurezza e certificazione di eventuali software di uso della CIE che il Comune volesse distribuire, anche via WEB, direttamente ai cittadini.

1) **Abilitazione di una postazione di lavoro all'identificazione in rete della CIE: processo elementare di comunicazione. Il responsabile del progetto CIE pubblica sul sito Comunale della CIE l'indirizzo del sito del CNSD da cui i cittadini possono scaricare il software per il riconoscimento in rete tramite CIE.**

   Asset individuati:
   a. Informazioni
      i. Il sito web del Comune per il riconoscimento tramite CIE
      ii. Le indicazioni del Ministero dell'Interno sulle modalità di accesso ai servizi distribuiti per la verifica della validità dei certificati digitali e delle informazioni anagrafiche memorizzati sulle CIE.
   b. Reti
      i. Le reti dati del Comune sulle quali transitano gli asset informativi individuati.
   c. Infrastrutture
      i. Le strutture che ospitano il sito WEB comunale per il riconoscimento in rete dei cittadini dotati di CIE..
   d. Hardware
      i. I sistemi che ospitano il WEB server del Comune
   e. Software
      i. Il WEB server del Comune
      ii. I software di verifica e riconoscimento resi disponibili dal Ministero dell'Interno

f. Risorse umane
   i. Il Sindaco
   ii. Il responsabile CIE.

4.3.2. Abilitazione di un server comunale per l'identificazione in rete dei cittadini che accedono tramite CIE ai servizi in rete del Comune

Si illustrano di seguito le fasi che devono essere svolte per abilitare un server comunale all'identificazione di un cittadino tramite CIE.

CONTROLLI:

Deve essere prestata particolare attenzione:

- Al fatto che, ai fini del riconoscimento in rete del cittadino attraverso la CIE, è sufficiente il solo certificato di sicurezza presente sulla CIE e non è quindi necessario che i dati anagrafici del cittadino siano inviati in rete.
  È infatti possibile per i WEB server autorizzati, nell'ambito dei servizi distribuiti del CNSD per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche, richiedere direttamente al Ministero dell'Interno i dati anagrafici sintetici associati ad un particolare certificato digitale CIE.
- Alla sicurezza e certificazione di eventuali software dedicati a specifici usi della CIE che il Comune volesse distribuire, anche via WEB, direttamente ai cittadini.

1) **Abilitazione di un server comunale per l'identificazione in rete dei cittadini che accedono tramite CIE: processo elementare di comunicazione**.
   Il responsabile del progetto CIE richiede al Ministero dell'Interno di poter accedere, attraverso la porta di accesso comunale, ai servizi distribuiti del CNSD per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE.

Asset individuati

a. Informazioni
   i. Il sito web del Comune per il riconoscimento tramite CIE
   ii. Le indicazioni del Ministero dell'Interno sulle modalità di accesso ai servizi distribuiti per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE.
   iii. L'autorizzazione del Ministero dell'Interno all'accesso ai servizi distribuiti del CNSD per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE.
   iv. Il servizio CNSD di Convalida INA
b. Reti
   i. Le reti di comunicazione verso la Porta di accesso ai domini applicativi del CNSD.
   ii. Le reti di comunicazione tra la Porta di accesso ai domini applicativi del CNSD ed il CNSD stesso.

c. Infrastrutture
    i. Le strutture organizzative utilizzate per la realizzazione dei software utilizzati a livello del server comunale.
d. Hardware
    i. I sistemi che ospitano il WEB server del Comune
    ii. La Porta comunale di accesso ai domini applicativi del CNSD
e. Software
    i. Il WEB server del Comune
f. Risorse umane
    i. Il Sindaco
    ii. Il responsabile CIE.
    iii. Le strutture organizzative che hanno realizzato le applicazioni informatiche per accedere ai servizi del CNSD.
    iv. Gli operatori incaricati della gestione del sito web comunale.

Allegato 4
SCHEDE DI ATTUAZIONE DELLA VERSIONE ALFA DEL PIANO SICUREZZA DEI COMUNI: CLASSIFICAZIONE MINACCE, VULNERABILITÀ E VALUTAZIONE DEL RISCHIO

1. Introduzione

Le schede di classificazione delle minacce e delle vulnerabilità, di seguito riportate, devono essere compilate per tutti gli asset associati ai processi elementari descritti nell'allegato 3, al fine di:

1) Individuare le vulnerabilità presenti nei sistemi tecnici ed organizzativi comunali.
2) Individuare, a fronte di queste vulnerabilità, le minacce per gli asset individuati.
3) Associare, per ogni terna "asset, vulnerabilità, minaccia", un livello di rischio.

Il Comune deve completare tali tabelle, introducendo eventualmente nuovi asset, vulnerabilità e minacce e valutando, rispetto ai propri modelli tecnici ed organizzativi, i livelli di rischio associati.

2. Schede di classificazione delle minacce e delle vulnerabilità

Le schede devono essere compilate dal responsabile sicurezza CIE del Comune che, per ogni processo elementare e per ogni asset indicato, deve inserire le vulnerabilità individuate e le minacce potenziali.

Nei successivi capitoli "3 – Minacce" e "4 – Vulnerabilità" sono forniti: un elenco delle principali minacce, in correlazione all'effetto che il loro avverarsi ha sulla sicurezza dell'informazione, ed un elenco delle vulnerabilità più diffuse.

Terminata la compilazione di tali schede, il Comune ottiene la prima parte del suo piano di sicurezza (versione alfa).
Si passa quindi alla successiva fase di **Valutazione del rischio**.
Nelle relative schede non vanno riportate quelle voci (processi elementari ed asset), presenti nelle schede precedenti, che non sono correlate ad alcuna minaccia potenziale.

Tali schede saranno utilizzate per la successiva valutazione dell'incidenza delle minacce individuate sugli asset dei processi elementari.
Nel capitolo successivo, si forniscono gli strumenti operativi per procedere alla valutazione del rischio.

Schede di classificazione delle minacce e delle vulnerabilità

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Acquisizione delle "quantità di sicurezza, attivazione e certificazione"		1) Nomina del responsabile comunale per la sicurezza degli accessi al CNSD.
ID	Classi	Asset	Minacce	Vulnerabilità
1	Informazioni	Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD.		
2	Informazioni	Direttive del Ministero dell'Interno		
3	Reti	-		
4	Infrastrutture…	Gli uffici comunali incaricati della custodia degli atti		
5	Hardware	-		
6	Software	-		
7	Risorse Umane	Il Sindaco		
8	Risorse Umane	Il responsabile comunale per la sicurezza degli accessi al CNSD		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Acquisizione delle "quantità di sicurezza, attivazione e certificazione"		2) Richiesta al Ministero dell'Interno delle "Quantità di sicurezza, attivazione e certificazione" e comunicazione ufficiale, al medesimo, del responsabile comunale per la sicurezza degli accessi al CNSD
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD		
2	**Informazioni**	Atto contenente la richiesta delle "Quantità di sicurezza, attivazione e certificazione"		
3	**Informazioni**	-		
4	**Informazioni**	-		
5	**Reti**	-		
6	**Infrastrutture…**	Gli uffici comunali incaricati della custodia degli atti.		
7	**Hardware**	-		
8	**Software**	-		
9	**Risorse Umane**	Il Sindaco		
10	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		
11	**Risorse Umane**	L'incaricato dell'invio al Ministero dell'Interno della richiesta delle "Quantità di sicurezza, attivazione e certificazione".		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Acquisizione delle "quantità di sicurezza, attivazione e certificazione"**		**3) Ricezione dei certificati digitali per accedere allo specifico sito WEB del CNSD dedicato alla registrazione dei responsabili comunali per la sicurezza degli accessi al CNSD per completare la richiesta delle "Quantità di sicurezza, attivazione e certificazione"**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD		
2	**Informazioni**	I certificati digitali per accedere al sito WEB del CNSD dedicato alla registrazione dei responsabili comunali per il completamento della richiesta delle "quantità di sicurezza, attivazione e certificazione"		
3	**Reti**	-		
4	**Infrastrutture**	Gli uffici comunali incaricati della custodia degli atti .		
5	**Infrastrutture**	Gli uffici comunali incaricati della custodia dei certificati digitali, predisposti dal Ministero dell'Interno, per l'accesso al sito WEB di registrazione, presso il CSND		
6	**Hardware**	-		
7	**Software**	-		
8	**Risorse Umane**	Il Sindaco		
9	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Acquisizione delle "quantità di sicurezza, attivazione e certificazione"		4) Completamento della richiesta delle "Quantità di sicurezza, attivazione e certificazione"
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Atti di nomina del responsabile comunale per la sicurezza degli accessi al CNSD		
2	**Informazioni**	I certificati digitali per accedere al sito WEB di registrazione presso il CNSD		
3	**Reti**	Le reti comunali attraverso cui transitano i flussi informativi per il completamento della registrazione del responsabile comunale		
4	**Infrastrutture**	Gli uffici comunali incaricati della custodia degli atti .		
5	**Infrastrutture**	Gli uffici comunali incaricati della custodia dei certificati digitali per l'accesso al sito WEB di registrazione, presso il CSND		
6	**Hardware**	-		
7	**Software**	-		
8	**Risorse Umane**	Il Sindaco		
9	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		

MACROPROCESSO	PROCESSO			ATTIVITÀ
Caricamento dell'INA	Acquisizione delle "quantità di sicurezza, attivazione e certificazione"			5) Il Comune riceve dal Ministero dell'Interno le "Quantità di sicurezza, attivazione e certificazione" per cui ha fatto precedentemente richiesta: processo elementare di comunicazione

ID	Classi	Asset	Minacce	Vulnerabilità
1	**Informazioni**	Atto di richiesta della "Quantità di sicurezza, attivazione e certificazione".		
2	**Informazioni**	Le "Quantità di sicurezza, attivazione e certificazione"		
3	**Reti**	Le reti di comunicazione del Comune		
4	**Infrastrutture…**	Gli uffici comunali incaricati della presa in carico delle "Quantità di sicurezza, attivazione e certificazione" e dell'eventuale trasporto verso il luogo di custodia .		
5	**Hardware**	-		
6	**Software**	-		
7	**Risorse Umane**	Il Sindaco		
8	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		
9	**Risorse Umane**	L'incaricato della presa in carico "Quantità di sicurezza, attivazione e certificazione".		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Acquisizione delle "quantità di sicurezza, attivazione e certificazione"**		**4) Il Comune deposita le "Quantità di sicurezza, attivazione e certificazione" ricevute dal Ministero dell'Interno presso una sede idonea al deposito di carte valori: processo elementare di Back office.**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	La "Quantità di sicurezza, attivazione e certificazione".		
2	**Informazioni**	Gli atti che indicano chi è responsabile della gestione dell'ufficio in cui sono depositate le "Quantità di sicurezza, attivazione e certificazione".		
3	**Reti**	Le reti comunali coinvolte nei flussi informativi connessi al processo di deposito delle "Quantità di sicurezza, attivazione e certificazione".		
4	**Infrastrutture…**	Gli uffici comunali incaricati della presa in carico delle "Quantità di sicurezza, attivazione e certificazione" e dell'eventuale trasporto al deposito.		
5	**Hardware**	-		
6	**Software**	-		
7	**Risorse Umane**	Il Sindaco		
8	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		
9	**Risorse Umane**	L'incaricato della presa in carico delle "Quantità di sicurezza, attivazione e certificazione".		
10	**Risorse Umane**	L'incaricato del deposito delle "Quantità di sicurezza, attivazione e certificazione".		

MACROPROCESSO	PROCESSO	ATTIVITÀ
Caricamento dell'INA	**Predisposizione Porta di Accesso ai Domini applicativi del CNSD**	**1) Installazione e prima configurazione dell'hardware e del software di base della porta di accesso del Comune, in base alle regole tecniche indicate dal Ministero dell'Interno: processo elementare di back office**

ID	Classi	Asset	Minacce	Vulnerabilità
1	**Informazioni**	Indicazioni sulle caratteristiche del software di base della porta di accesso, fornite dal Ministero dell'Interno		
2	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali .		
3	**Reti**	-		
4	**Infrastrutture**	La sede ove il Comune installa la Porta di accesso ai domini applicativi del CNSD.		
5	**Hardware**	I sistemi hardware utilizzati per la porta di accesso ai domini applicativi del CNSD.		
6	**Software**	Il software di base della Porta di accesso ai domini applicativi del CNSD.		
7	**Risorse Umane**	Il responsabile dei Sistemi Informatici del Comune		
8	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Predisposizione Porta di Accesso ai Domini applicativi del CNSD**		**2) Configurazione dell'infrastruttura di rete comunale: attività di back office per la configurazione delle sezioni di rete comunale necessarie alle comunicazioni tra la porta di accesso ed il CNSD**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Direttive ed indicazioni del Ministero dell'Interno		
2	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali .		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD.		
5	**Infrastrutture…**	La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati.		
6	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD.		
7	**Software**	-		
8	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
9	**Risorse Umane**	Il responsabile delle reti del Comune		
10	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		

MACROPROCESSO	PROCESSO			ATTIVITÀ
Caricamento dell'INA	**Predisposizione Porta di Accesso ai Domini applicativi del CNSD**			**3) Installazione della porta di accesso ai domini del CNSD, utilizzando le "quantità di sicurezza, attivazione e certificazione", attivazione Backbone CNSD, attivazione degli agenti di monitoraggio ed allarmi: processo elementare di back office**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali.		
2	**Informazioni**	"quantità di sicurezza, attivazione e certificazione", e software della Porta di accesso ai domini applicativi del CNSD, predisposti dal Ministero dell'Interno.		
3	**Reti**	Le reti di comunicazione dati del Comune per le comunicazioni verso la porta di accesso e, attraverso questa, verso il CNSD		
4	**Infrastrutture**	La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati.		
5	**Infrastrutture**	La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".		
6	**Infrastrutture**	Gli uffici eventualmente incaricati del trasporto delle "Quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede in cui è stata installata la Porta di accesso ai domini applicativi del CNSD.		
7	**Hardware**	I supporti su cui sono memorizzate le "quantità di sicurezza, attivazione e certificazione" ed il software della Porta di accesso ai domini applicativi del CNSD.		
8	**Hardware**	Il computer (pc, server, …) su cui installare il software della Porta di accesso ai domini applicativi del CNSD		
9	**Hardware**	I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD		
10	**Software**	Il software della Porta di accesso ai domini applicativi del CNSD		
11	**Software**	Gli agenti software di monitoraggio ed allarme		
12	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
13	**Risorse Umane**	Il responsabile dei sistemi di rete del Comune		
14	**Risorse Umane**	Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD		
15	**Risorse Umane**	I tecnici che devono installare la Porta di accesso ai domini applicativi del CNSD.		
16	**Risorse Umane**	Il call center del CNSD supporta e verifica la corretta installazione della Porta di accesso ai domini applicativi del CNSD.		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Caricamento dell'INA		**Predisposizione Porta di Accesso ai Domini applicativi del CNSD**		**4) Verifica di funzionamento e collegamento in rete della porta di accesso ai domini applicativi del CNSD e, in caso positivo, attivazione della porta stessa: processo elementare di back office.**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	"Quantità di sicurezza, attivazione e certificazione.		
4	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD.		
5	**Infrastrutture**	La sede presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".		
6	**Infrastrutture**	Gli uffici eventualmente incaricati del trasporto delle "quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede in cui è installata la porta di accesso ai domini applicativi del CNSD.		
7	**Infrastrutture…**	La sede/i presso cui il Comune ha installato la porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati		
8	**Hardware**	Il computer (pc, server, …) su cui è installato il software della Porta di accesso ai domini applicativi del CNSD.		
9	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune alla porta di accesso e, tramite questa, al CNSD.		
10	**Software**	Il software della porta di accesso ai domini applicativi del CNSD e le relative applicazioni software di supporto		
11	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
12	**Risorse Umane**	Il responsabile dei sistemi di rete del Comune		
13	**Risorse Umane**	Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD		
14	**Risorse Umane**	L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".		
15	**Risorse Umane**	Il Call center del CNSD che fornisce supporto all'esecuzione delle verifiche di funzionamento e connessione in rete per l'attivazione operativa della Porta di accesso ai domini applicativi del CNSD.		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi INA del CNSD		1) Registrazione del sistema comunale sulla porta di accesso ai domini applicativi del CNSD: processo elementare di back office
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	"quantità di sicurezza, attivazione e certificazione".		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Infrastrutture**	La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".		
5	**Infrastrutture**	Gli uffici eventualmente incaricati del trasporto della "quantità di sicurezza, attivazione e certificazione"dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
6	**Infrastrutture**	La sede/i presso cui il Comune ha installato la Porta di accesso ai domini applicativi del CNSD e gli apparati di rete e di sicurezza collegati		
7	**Infrastrutture**	Le sedi in cui sono installati i sistemi comunali che devono essere messi in comunicazione con la porta di accesso		
8	**Hardware**	Il computer (pc, server, ...) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.		
9	**Hardware**	L'hardware dei sistemi comunali da collegare alla porta di accesso		
10	**Hardware**	I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
11	**Software**	L'applicativo software per la registrazione e l'attivazione di comunicazioni in rete crittografate in base a certificati digitali, contenuto nelle "quantità di sicurezza, attivazione e certificazione, ed installato sui sistemi comunali che devono essere collegati alla porta di accesso		
12	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
13	**Risorse Umane**	Il responsabile dei sistemi di rete del Comune		
14	**Risorse Umane**	Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD		
15	**Risorse Umane**	L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".		
16	**Risorse Umane**	Il Call center del CNSD che fornisce supporto ai Comuni per la registrazione dei sistemi comunali alla Porta di accesso ai domini applicativi del CNSD		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi INA del CNSD		2) Verifica della corretta configurazione delle comunicazioni tra i sistemi comunali e la porta di accesso ai domini applicativi del CNSD: processo elementare di back office.
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	"Quantità di sicurezza, attivazione e certificazione"		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD.		
5	**Infrastrutture**	La sede/i presso cui il Comune conserva le "quantità di sicurezza, attivazione e certificazione".		
6	**Infrastrutture**	Gli uffici eventualmente incaricati del trasporto delle "quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD.		
7	**Infrastrutture**	La sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
8	**Infrastrutture**	Le sedi in cui sono installati i sistemi comunali che devono essere messi in comunicazione con la porta di accesso.		
9	**Hardware**	Il computer (pc, server, …) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.		
10	**Hardware**	L'hardware dei sistemi comunali da collegare alla porta di accesso.		
11	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.		
12	**Software**	L'applicativo software per la verifica delle comunicazioni certificate tra i sistemi comunali e la porta di accesso		
13	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
14	**Risorse Umane**	Il responsabile dei sistemi di rete del Comune		
15	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		
16	**Risorse Umane**	L'incaricato del deposito delle "quantità di sicurezza, attivazione e certificazione".		
17	**Risorse Umane**	Il Call center del CNSD che fornisce supporto nelle verifiche della sussistenza e completezza delle comunicazioni tra i sistemi comunali e la Porta di accesso ai domini applicativi del CNSD e tra quest'ultima ed il CNSD		

MACROPROCESSO	PROCESSO	ATTIVITÀ
Caricamento dell'INA	**Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria**	**1) Il Comune estrae dalla propria anagrafe le corrispondenze tra dati anagrafici e codici fiscali, ivi compresi i dati anagrafici ai quali non è associato un codice fiscale: processo elementare di elaborazione**

ID	Classi	Asset	Minacce	Vulnerabilità
1	**Informazioni**	Archivio anagrafico del Comune		
2	**Informazioni**	Archivio delle corrispondenze dato anagrafico-codice fiscale		
3	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
4	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
5	**Infrastrutture…**	La/e sede/i comunale/i dell'archivio anagrafico comunale		
6	**Infrastrutture…**	La/e sede/i comunale/i presso cui l'archivio delle corrispondenze viene depositato		
7	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze		
8	**Hardware**	Il/i sistema/i comunale/i di gestione ed archiviazione dei dati anagrafici		
9	**Hardware**	Il/i terminale/i da cui si accede all'anagrafe per attivare la procedura di estrazione dell'archivio delle corrispondenze		
10	**Hardware**	I dispositivi di memorizzazione dell'archivio delle corrispondenze		
11	**Hardware**	La porta di accesso ai domini applicativi del CNSD		
12	**Software**	Il Sistema Informativo Comunale		
13	**Software**	I servizi d'estrazione dei dati anagrafici dall'archivio anagrafico comunale		
14	**Software**	Il software d'estrazione delle corrispondenze		
15	**Software**	Il software di memorizzazione dell'archivio delle corrispondenze sui dispositivi hardware preposti		
16	**Risorse Umane**	Il responsabile dell'anagrafe		
17	**Risorse Umane**	Il responsabile del Sistema Informativo Comunale		
18	**Risorse Umane**	I tecnici informatici incaricati dell'attuazione del processo di estrazione e creazione dell'archivio delle corrispondenze		
19	**Risorse Umane**	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria**		**2) Il Comune, a partire dalle corrispondenze così ottenute, predispone un archivio utilizzando le specifiche definite dall'Anagrafe Tributaria: processo elementare di elaborazione**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
21	**Informazioni**	Archivio delle corrispondenze dato anagrafico - codice fiscale		
22	**Informazioni**	Archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria		
23	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
24	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
25	**Infrastrutture…**	La/e sede/i comunale/i presso cui è presente l'archivio delle corrispondenze		
26	**Infrastrutture…**	La/e sede/i comunale/i presso cui l'archivio predisposto per Anagrafe Tributaria viene depositato		
27	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze		
28	**Hardware**	Il/i terminale/i da cui si accede all'anagrafe per attivare la procedura di strutturazione dell'archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria		
29	**Hardware**	I dispositivi di memorizzazione dell'archivio delle corrispondenze		
30	**Hardware**	I dispositivi di memorizzazione dell'archivio predisposto nel formato richiesto dall'Anagrafe Tributaria		
31	**Software**	Il software di trasformazione dell'archivio delle corrispondenze nel formato richiesto dall'Anagrafe Tributaria		
32	**Software**	Il software di memorizzazione dell'archivio delle corrispondenze nel formato archivio richiesto da Anagrafe Tributaria sui dispositivi hardware preposti		
33	**Risorse Umane**	I tecnici informatici incaricati dell'attuazione del processo di trasformazione dell'archivio delle corrispondenze		
34	**Risorse Umane**	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze e dell'archivio trasformato nel formato richiesto da Anagrafe Tributaria		

ID	Classi	Asset	Minacce	Vulnerabilità
MACROPROCESSO Caricamento dell'INA		**PROCESSO** Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria		**ATTIVITÀ** 3) Il Comune invia l'archivio così formato all'Anagrafe Tributaria
35	**Informazioni**	Archivio delle corrispondenze nel formato richiesto da Anagrafe Tributaria		
36	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
37	**Informazioni**	Archivio delle "ricevute" fornite da Anagrafe Tributaria come conferma della ricezione dell'archivio delle corrispondenze anagrafe-codici fiscali		
38	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
39	**Reti**	La rete verso il CNSD e l'Anagrafe Tributaria		
40	**Infrastrutture**	La/e sede/i comunale/i presso cui l'archivio predisposto per Anagrafe Tributaria viene depositato		
41	**Infrastrutture**	La/e sede/i da cui il Comune trasmette i dati verso Anagrafe Tributaria		
42	**Infrastrutture**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviate le corrispondenze da consegnare ad Anagrafe Tributaria		
43	**Hardware**	Il/i terminale/i da cui si accede per inviare l'archivio delle corrispondenze in rete		
43	**Hardware**	La porta di accesso ai domini applicativi del CNSD per l'accesso al Backbone del CNSD, utilizzato per la certificazione e la sicurezza della trasmissione dell'archivio delle corrispondenze e delle relative ricevute da parte di Anagrafe Tributaria.		
44	**Hardware**	I dispositivi di memorizzazione dell'archivio delle corrispondenze		
45	**Hardware**	I dispositivi di memorizzazione dell'archivio delle "ricevute" di Anagrafe Tributaria		
46	**Software**	il software di invio dell'archivio delle corrispondenze verso Anagrafe Tributaria e di ricezione delle ricevute attraverso la Porta di accesso ai domini applicativi del CNSD ovvero direttamente ad Anagrafe Tributaria		
47	**Software**	Il Software di archiviazione delle ricevute di Anagrafe Tributaria		
48	**Risorse Umane**	I tecnici informatici incaricati dell'attuazione del processo di invio dell'archivio delle corrispondenze e della ricezione delle "ricevute" di Anagrafe Tributaria		
49	**Risorse Umane**	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze e dell'archivio delle ricevute di Anagrafe Tributaria		

MACROPROCESSO	PROCESSO	ATTIVITÀ
Caricamento dell'INA	**Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria**	**4) L'Anagrafe Tributaria verifica la coerenza dell'archivio, attribuisce o aggiorna i codici fiscali non presenti o non allineati, segnala le corrispondenze non assegnate. L'Anagrafe Tributaria invia al Comune l'archivio di corrispondenze aggiornato.**

ID	Classi	Asset	Minacce	Vulnerabilità
50	**Informazioni**	Archivio delle corrispondenze aggiornato da Anagrafe Tributaria		
51	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
52	**Informazioni**	Archivio delle "ricevute" fornite da Anagrafe Tributaria come conferma della ricezione dell'archivio delle corrispondenze anagrafe-codici fiscali		
53	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
	Reti	La rete verso il CNSD e l'Anagrafe Tributaria		
55	**Infrastrutture…**	La/e sede/i da cui il Comune riceve i dati allineati da Anagrafe Tributaria		
56	**Infrastrutture…**	La/e sede/i comunale/i presso cui l'archivio allineato da Anagrafe Tributaria viene depositato		
57	**Hardware**	Il/i terminale/i da cui si accede per ricevere l'archivio delle corrispondenze allineato da Anagrafe Tributaria		
58	**Hardware**	La Porta di accesso ai domini applicativi del CNSD per l'accesso al Backbone del CNSD, utilizzato per la certificazione e la sicurezza della ricezione dell'archivio delle corrispondenze allineate		
59	**Hardware**	I dispositivi di memorizzazione dell'archivio delle corrispondenze allineate		
60	**Hardware**	I dispositivi di memorizzazione dell'archivio delle "ricevute" di Anagrafe Tributaria		
61	**Software**	Il software di ricezione dell'archivio delle corrispondenze allineate da Anagrafe Tributaria attraverso la Porta di dominio comunale		
62	**Software**	il software di accesso alle ricevute di Anagrafe Tributaria		
63	**Software**	Il software di verifica della corrispondenza tra le ricevute di presa in consegna da parte di Anagrafe Tributaria degli archivi di corrispondenze non allineati con gli archivi delle corrispondenze allineate ricevuti da Anagrafe Tributaria		
64	**Risorse Umane**	I tecnici informatici incaricati dell'attuazione del processo di ricezione dell'archivio delle corrispondenze e verifica con le "ricevute" di Anagrafe Tributaria		
65	**Risorse Umane**	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze allineate e dell'archivio delle ricevute di Anagrafe Tributaria		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria		5) Il Comune, per ogni elemento dell'archivio di corrispondenze, aggiorna nella propria anagrafe le corrispondenze tra dato anagrafico e codice fiscale.
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
66	Informazioni	Archivio anagrafico del Comune		
67	Informazioni	Archivio delle corrispondenze aggiornato da Anagrafe Tributaria e verificato con l'archivio delle ricevute di Anagrafe Tributaria		
68	Informazioni	Archivio delle abilitazioni per l'uso dei sistemi comunali		
69	Reti	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
70	Infrastrutture…	La/e sede/i da cui il Comune elabora le corrispondenze allineate da Anagrafe Tributaria		
71	Infrastrutture…	La/e sede/i comunale/i presso cui l'archivio delle corrispondenze allineate da Anagrafe Tributaria è stato depositato		
72	Hardware	Il sistema informativo comunale		
73	Hardware	Il/i terminale/i da cui si accede per attivare la procedura di inserimento delle corrispondenze allineate nell'anagrafe comunale		
74	Hardware	I dispositivi di memorizzazione dell'archivio delle corrispondenze allineate		
75	Software	Il software di riallineamento dall'anagrafe comunale a partire dall'archivio delle corrispondenze allineato da Anagrafe Tributaria		
76	Risorse Umane	Il responsabile del Sistema informativo comunale		
77	Risorse Umane	Il responsabile dell'anagrafe		
78	Risorse Umane	I tecnici informatici incaricati dell'attuazione del processo di riallineamento		
79	Risorse Umane	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze allineate		

MACROPROCESSO	PROCESSO			ATTIVITÀ
Caricamento dell'INA	**Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria**			**6) Il Comune, per tutti i casi di non corrispondenza, inizia una serie di attività di recupero dei codici fiscali per le corrispondenze non assegnate dall'Anagrafe Tributaria.**

ID	Classi	Asset	Minacce	Vulnerabilità
80	**Informazioni**	Archivio anagrafico del comune		
81	**Informazioni**	Archivio dei dati anagrafici i cui codici fiscali non sono ancora allineati		
82	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
83	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
84	**Infrastrutture…**	La/e sede/i da cui il Comune elabora le corrispondenze non allineate da Anagrafe Tributaria		
85	**Infrastrutture…**	La/e sede/i comunale/i presso cui l'archivio delle corrispondenze non allineate da Anagrafe Tributaria è stato depositato		

86	**Hardware**	Il sistema informativo comunale		
87	**Hardware**	Il/i terminale/i da cui si accede per attivare la procedura di correzione delle corrispondenze non allineate nell'anagrafe comunale		
88	**Hardware**	I dispositivi di memorizzazione dell'archivio delle corrispondenze non allineate		
89	**Software**	Il software per la creazione e la gestione dell'archivio delle corrispondenze dato anagrafico - codice fiscale non ancora allineate		
90	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
91	**Risorse Umane**	Il responsabile dell'anagrafe		
92	**Risorse Umane**	I tecnici informatici incaricati dell'attuazione del processo di riallineamento		
93	**Risorse Umane**	Lo/gli incaricato/i del deposito dell'archivio delle corrispondenze non ancora allineate		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Primo caricamento dell'Indice Nazionale delle Anagrafi**		**1) Predisposizione dell'archivio anagrafico, nel formato previsto per il primo caricamento dell'Indice Nazionale delle Anagrafi, da inviare, attraverso la Porta di accesso ai domini applicativi del CNSD, al CNSD**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio anagrafico del Comune		
2	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Infrastrutture…**	Il sistema informativo comunale		
5	**Infrastrutture…**	La sede presso cui il Comune archivia l'archivio anagrafico per il primo caricamento dell'INA		
6	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui sono archiviati i dati di primo caricamento dell'INA dalla sede in cui sono stati estratti, alla sede in cui devono essere temporaneamente archiviati o alla sede destinata al successivo invio dei dati		
7	**Hardware**	Il sistema informativo comunale		
8	**Hardware**	Il terminale da cui è attivata la procedura di estrazione dei dati dall'anagrafe nel formato richiesto per il primo caricamento dell'INA		
9	**Software**	La procedura software per la strutturazione dei dati anagrafici nel formato richiesto dal primo caricamento dell'INA		
10	**Risorse Umane**	Il responsabile dei sistemi informatici del comune		
11	**Risorse Umane**	Il responsabile dell'anagrafe		
12	**Risorse Umane**	Lo/gli incaricato/i dell'archiviazione dell'archivio anagrafico da inviare successivamente all'INA		
13	**Risorse Umane**	L'operatore che attiva la procedura di formazione dell'archivio di primo caricamento dell'INA		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Primo caricamento dell'Indice Nazionale delle Anagrafi**		**2) Invio al CNSD dei dati anagrafici per il primo caricamento dell'INA**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	Archivio di primo caricamento dell'INA		
3	**Informazioni**	Ricevuta dell'invio effettuato		
4	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
5	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD		
6	**Infrastrutture…**	La sede/i presso cui il Comune ha archiviato l'archivio di primo caricamento dell'INA		
7	**Infrastrutture…**	La sede del Comune presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
8	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato il primo caricamento dell'INA dalla sede di archiviazione alla sede di invio al CNSD		
9	**Hardware**	La Porta di accesso ai domini applicativi del CNSD		
10	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
11	**Software**	La Porta di accesso ai domini applicativi del CNSD		
12	**Software**	Il software di invio al CNSD dell'archivio del primo caricamento dell'INA		
13	**Risorse Umane**	Il responsabile delle reti		
14	**Risorse Umane**	Il responsabile della Porta di accesso ai domini applicativi del CNSD		
15	**Risorse Umane**	Lo/gli incaricato/i del trattamento dell'archivio relativo al primo caricamento dell'INA		
16	**Risorse Umane**	Lo/gli incaricato/i dell'archiviazione delle ricevute, fornite dal CNSD, di invio effettuato		
17	**Risorse Umane**	Lo/gli incaricato/i dell'invio al CNSD del primo caricamento dell'INA e dell'acquisizione della ricevuta di invio effettuato		
18	**Risorse Umane**	Il Call center del CNSD a supporto delle operazioni di invio al CNSD		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Aggiornamento continuo dell'Indice Nazionale delle Anagrafi		1) Acquisizione ed installazione del software di supporto all'invio delle variazioni anagrafiche al CNSD
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
3	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD		
4	**Infrastrutture…**	La sede/i presso cui il Comune archivia il software di invio delle variazioni anagrafiche ricevuto dal Ministero dell'interno		
5	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato il software di invio delle variazioni anagrafiche		
6	**Hardware**	Il terminale utilizzato per connettersi al CNSD per richiedere ed acquisire il software di invio delle variazioni anagrafiche.		
7	**Hardware**	I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
8	**Software**	Il software di supporto all'invio delle variazioni anagrafiche nei formati XML o XML SOAP		
9	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
10	**Risorse Umane**	Il responsabile delle reti		
11	**Risorse Umane**	Il responsabile della Porta di accesso ai domini applicativi del CNSD		
12	**Risorse Umane**	Lo/gli incaricato/i di archiviare il software ricevuto dal Ministero dell'Interno		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		Aggiornamento continuo dell'Indice Nazionale delle Anagrafi		2) Predisposizione dell'archivio contenente le variazioni anagrafiche da inviare al CNSD per l'aggiornamento dell'INA
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	Archivio anagrafico		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Infrastrutture…**	La sede/i dell'archivio anagrafico		
5	**Infrastrutture…**	La sede del Comune presso cui depositare temporaneamente l'archivio di aggiornamento dell'INA		
6	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici tra le sedi coinvolte		
7	**Hardware**	I sistemi informatici del Comune		
8	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
9	**Software**	Il Sistema Informativo Comunale		
10	**Software**	La procedura software di estrazione e strutturazione in uno dei formati richiesti, degli aggiornamento anagrafici da inviare al CNSD		
11	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
12	**Risorse Umane**	Il responsabile dell'anagrafe		
13	**Risorse Umane**	Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA		
14	**Risorse Umane**	L'operatore incaricato dell'attivazione della procedura di formazione dell'archivio di aggiornamento dell'INA da inviare al CNSD		
15	**Risorse Umane**	Il Call center del CNSD a supporto dei comuni		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Caricamento dell'INA		**Aggiornamento continuo dell'Indice Nazionale delle Anagrafi**		**3) Invio al CNSD dell'archivio delle variazioni anagrafiche per l'aggiornamento dell'INA**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
29	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
30	**Informazioni**	Archivio di aggiornamento dell'INA		
30	**Informazioni**	Ricevuta, fornita dal CNSD, dell'invio effettuato		
31	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
32	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD		
33	**Infrastrutture…**	La sede/i presso cui il Comune ha depositato l'archivio di aggiornamento dell'INA		
34	**Infrastrutture…**	La sede da cui il Comune effettua l'invio dell'aggiornamento INA al CNSD attraverso la porta di accesso		
34	**Infrastrutture…**	La sede del Comune presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
34	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato l'aggiornamento dell'INA dalla sede di archiviazione alla sede di invio al CNSD.		
35	**Hardware**	La Porta di accesso ai domini applicativi del CNSD		
36	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
37	**Software**	La Porta di accesso ai domini applicativi del CNSD		

37	**Software**	Il software per l'invio al CNSD, attraverso la Porta di accesso ai domini applicativi dello stesso, dell'aggiornamento dell'INA oppure, fino al 31/12/2005, il software PCCSA		
39	**Risorse Umane**	Il responsabile delle reti		
40	**Risorse Umane**	Il responsabile della Porta di accesso ai domini applicativi del CNSD		
40	**Risorse Umane**	Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA		
41	**Risorse Umane**	Lo/gli incaricato/i dell'archiviazione delle ricevute, fornite dal CNSD, dell'invio effettuato		
41	**Risorse Umane**	L'operatore incaricato dell'invio al CNSD dell'aggiornamento dell'INA e dell'acquisizione della ricevuta di invio effettuato		
41	**Risorse Umane**	Il Call center del CNSD a supporto dei Comuni		

MACROPROCESSO	PROCESSO	ATTIVITÀ
Caricamento dell'INA	**Aggiornamento in continua dell'Indice Nazionale delle Anagrafi**	**4) Predisposizione dell'archivio contenente le variazioni anagrafiche da inviare al CNSD per l'aggiornamento dell'INA**

ID	Classi	Asset	Minacce	Vulnerabilità
42	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
43	**Informazioni**	Archivio anagrafico		
44	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi		
45	**Infrastrutture…**	La sede/i dell'archivio anagrafico		
46	**Infrastrutture…**	La sede del Comune presso cui depositare temporaneamente l'archivio di aggiornamento dell'INA		
47	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici tra le sedi coinvolte		

48	**Hardware**	Il sistema informatico comunale		
49	**Software**	Il sistema informatico comunale		
50	**Software**	La procedura software di estrazione e strutturazione in uno dei formati richiesti, degli aggiornamento anagrafici da inviare al CNSD		
51	**Risorse Umane**	Il responsabile del sistema informatico comunale		
52	**Risorse Umane**	Il responsabile dell'anagrafe		
53	**Risorse Umane**	Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA		
54	**Risorse Umane**	L'operatore incaricato dell'attivazione della procedura di formazione dell'archivio con gli aggiornamenti per l'INA da inviare al CNSD		
55	**Risorse Umane**	Il Call center del CNSD a supporto dei comuni		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Caricamento dell'INA		**Aggiornamento in continua dell'Indice Nazionale delle Anagrafi**		**5) Invio al CNSD dell'archivio delle variazioni anagrafiche per l'aggiornamento dell'INA**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
56	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
57	**Informazioni**	Archivio di aggiornamento dell'INA		
58	**Informazioni**	Ricevuta, fornita dal CNSD, di invio effettuato		
59	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
60	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD		

61	**Infrastrutture…**	La sede/i presso cui il Comune ha archiviato l'archivio di aggiornamento dell'INA		
62	**Infrastrutture…**	La sede da cui il Comune effettua l'invio dell'aggiornamento INA al CNSD		
63	**Infrastrutture…**	La sede del Comune presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
64	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto dei supporti fisici su cui è archiviato l'aggiornamento dell'INA dalla sede di archiviazione alla sede di invio al CNSD		
65	**Hardware**	La Porta di accesso ai domini applicativi del CNSD		
66	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD		
67	**Software**	La Porta di accesso ai domini applicativi del CNSD		
68	**Software**	Il software PCCSA, ovvero il software WEB HTTP per l'invio attraverso la Porta di accesso ai domini applicativi del CNSD, dell'aggiornamento dell'INA al CNSD		
69	**Risorse Umane**	Il responsabile delle reti		
70	**Risorse Umane**	Il responsabile della Porta di accesso ai domini applicativi del CNSD		
71	**Risorse Umane**	Lo/gli incaricato/i del trattamento dell'archivio contenente l'aggiornamento dell'INA		
72	**Risorse Umane**	Lo/gli incaricato/i dell'archiviazione delle ricevute, fornite dal CNSD, di invio effettuato		
73	**Risorse Umane**	L'operatore incaricato dell'invio al CNSD dell'aggiornamento dell'INA e della ricezione della ricevuta di invio effettuato		
74	**Risorse Umane**	Il Call center del CNSD a supporto dei Comuni		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Nomina del responsabile della CIE**		**1) Il Sindaco nomina il responsabile comunale della sicurezza CIE denominato anche responsabile CIE**

ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Atti di nomina del responsabile della CIE.		
2	**Informazioni**	Direttive del Ministero dell'Interno		
3	**Reti**	-		
4	**Infrastrutture…**	Le strutture organizzative adibite alla custodia degli atti.		
5	**Hardware**	-		
6	**Software**	-		
7	**Risorse Umane**	Il Sindaco		
8	**Risorse Umane**	Il responsabile comunale per la sicurezza degli accessi al CNSD		
9	**Risorse Umane**	Il responsabile della CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Predisposizione della Postazione di Emissione**		**1) Il Comune installa presso le sedi designate le postazioni di emissione**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	-		
3	**Reti**	Le reti dati del Comune alle quali collegare le postazioni di emissione		
3	**Reti**	La rete presso cui è installata la Porta di accesso ai domini applicativi del CNSD di accesso al backbone del CNSD		
3	**Reti**	La rete che consente alle postazioni di emissione di comunicare tra loro, di comunicare con la Porta di accesso ai domini applicativi del CNSD e, attraverso questo, di comunicare con il SSCE		
3	**Reti**	La protezione fisica dei dispositivi di rete attraverso cui passano le comunicazioni delle postazioni di emissione verso la Porta di accesso ai domini applicativi del CNSD e da questa verso il CNSD		
4	**Infrastrutture…**	li uffici comunali ove sono installate le postazioni di emissione		
5	**Hardware**	La protezione fisica delle postazioni di emissione e della Porta di accesso ai domini applicativi del CNSD e di tutti gli apparati (lettore/scrittore di chip, stampante termica e relativo lettore di chip, lettore/scrittore di banda laser,…) ad esse connesse		
6	**Software**	-		
7	**Risorse Umane**	Il responsabile della CIE		
8	**Risorse Umane**	Gli operatori ed i tecnici incaricati di installare gli apparati di emissione e di configurare il relativo software di base		
9	**Risorse Umane**	Il Call Center CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Attivazione delle Postazioni di Emissione ai servizi applicativi di emissione CIE del CNSD**		**1) Abilitazione del sistema all'accesso del servizio applicativo del CNSD tramite "quantità di sicurezza, attivazione e certificazione": processo elementare di back office per attivazione agenti di monitoraggio ed allarmi**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	"quantità di sicurezza, attivazione e certificazione".		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD.		
5	**Infrastrutture…**	La sede/i comunale che ospita/no le postazioni di emissione.		
6	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto delle "Quantità di sicurezza, attivazione e certificazione" dalla sede di deposito alla sede/i in cui sono state installate le postazioni di emissione		
7	**Infrastrutture…**	iii. La/e sede/i presso cui sono installate le postazioni di emissione		
8	**Hardware**	Hardware delle postazioni di emissione.		
10	**Hardware**	i dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni relative all'emissione di CIE.		
11	**Software**	Il software di emissione CIE		
12	**Software**	Il software degli Agenti di monitoraggio ed allarmi.		
13	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
14	**Risorse Umane**	Il responsabile delle reti		
15	**Risorse Umane**	Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD		
16	**Risorse Umane**	Il responsabile della CIE		
17	**Risorse Umane**	I tecnici che gestiscono i sistemi comunali.		
18	**Risorse Umane**	Lo/gli incaricato/i del deposito delle "quantità di sicurezza, attivazione e certificazione".		
19	**Risorse Umane**	Il call center del CNSD che supporta i tecnici comunali nell'attivazioend egli agenti di monitoraggio ed allarmi.		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Attivazione delle Postazioni di Emissione ai servizi applicativi di emissione CIE del CNSD		2) verifica della corretta configurazione dei canali di comunicazione.
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
2	**Informazioni**	"Quantità di sicurezza, attivazione e certificazione"		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati.		
4	**Reti**	La rete dati del Comune per le comunicazioni verso il CNSD.		
5	**Infrastrutture…**	La sede presso cui il Comune deposita la "quantità di sicurezza, attivazione e certificazione".		
6	**Infrastrutture…**	Le strutture operative eventualmente incaricate del trasporto della "quantità di sicurezza, attivazione e certificazione"dalla sede di deposito alla sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD.		
7	**Infrastrutture…**	La sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
8	**Infrastrutture…**	La/e sede/i presso cui sono installate le postazioni di emissione		
9	**Hardware**	Il computer (pc, server, …) su cui è stata installata la Porta di accesso ai domini applicativi del CNSD.		
10	**Hardware**	Hardware delle postazioni di emissione		
11	**Hardware**	I dispositivi di rete: router, firewall, proxy, sui quali transitano le comunicazioni in rete dal Comune al CNSD.		
12	**Software**	Gli strumenti software per le verifiche di connettività, contenuti nelle "quantità di sicurezza, attivazione e certificazione"		
14	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
15	**Risorse Umane**	Il responsabile dei sistemi di rete del Comune		
16	**Risorse Umane**	Il responsabile comunale per la sicurezza delle comunicazioni con il CNSD		
17	**Risorse Umane**	Il responsabile della CIE		
18	**Risorse Umane**	Lo/gli incaricato/i del deposito delle "quantità di sicurezza, attivazione e certificazione".		
19	**Risorse Umane**	Il Call center del CNSD che fornisce supporto per la corretta esecuzione delle verifiche di comunicazione.		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Acquisizione delle Quantità di sicurezza**		**1) Richiesta delle Quantità di Sicurezza al Ministero dell'Interno**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Richiesta delle Quantità di Sicurezza.		
2	**Informazioni**	Gli atti di nomina del responsabile dell'invio delle richieste al Ministero dell'Interno.		
	Informazioni	Direttive del Ministero dell'Interno		
3	**Reti**	Le reti comunali coinvolte nei flussi informativi connessi all'effettuazione della richiesta.		
4	**Infrastrutture…**	-		
5	**Hardware**	Nessuno		
6	**Software**	Nessuno		
7	**Risorse Umane**	Il Sindaco		
8	**Risorse Umane**	Il responsabile della CIE		
9	**Risorse Umane**	Lo/gli incaricato/i dell'effettuazione della richiesta		
10	**Risorse Umane**	Il call center CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Acquisizione delle Quantità di sicurezza**		**2) Il Comune riceve dal Ministero dell'Interno le quantità di Sicurezza per cui ha fatto precedentemente richiesta: processo elementare di comunicazione**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Richiesta delle Quantità di Sicurezza.		
2	**Informazioni**	Gli atti di nomina del responsabile della presa in carico delle quantità di sicurezza.		
3	**Informazioni**	Atti relativi alla presa in carico delle quantità di sicurezza		
4	**Reti**	-		
5	**Infrastrutture**	Le strutture organizzative adibite alla presa in carico delle quantità di sicurezza ed all'eventuale trasporto verso il luogo di custodia.		
6	**Hardware**	Nessuno		
7	**Software**	Nessuno		
8	**Risorse Umane**	Il Sindaco		
9	**Risorse Umane**	Il responsabile della CIE		
10	**Risorse Umane**	Lo/gli incaricato/i della presa in carico delle quantità di sicurezza.		
11	**Risorse Umane**	Il call center CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Acquisizione della Quantità di sicurezza		3) Il Comune deposita le quantità di sicurezza ricevute dal Ministero dell'Interno presso una sede idonea al deposito di carte valori: processo elementare di Back office.
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Le quantità di sicurezza.		
2	**Informazioni**	Gli atti di nomina dei responsabili del deposito e della gestione dei relativi locali.		
3	**Reti**	-.		
4	**Infrastrutture…**	Le strutture organizzative adibite alla presa in carico delle quantità di sicurezza presso il deposito ed all'eventuale trasporto al deposito stesso		
5	**Hardware**	Nessuno		
6	**Software**	Nessuno		
7	**Risorse Umane**	Il Sindaco		
8	**Risorse Umane**	Il responsabile della CIE		
9	**Risorse Umane**	Lo/gli incaricato/i della presa in carico delle quantità di sicurezza.		
10	**Risorse Umane**	Lo/gli incaricato/i del deposito delle quantità di sicurezza.		
11	**Risorse Umane**	Il call center CIE.		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Acquisizione delle CIE inizializzate		*1) Il Comune richiede un lotto di CIE al Ministero dell'Interno: processo elementare di comunicazione*
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
21	**Informazioni**	Il numero di CIE richieste		
22	**Informazioni**	Gli atti di nomina del responsabile dell'invio delle richieste al Ministero dell'Interno.		
23	**Reti**	-		
24	**Infrastrutture…**	-		
25	**Hardware**	Nessuno		
26	**Software**	Nessuno		
27	**Risorse Umane**	Il Sindaco		
28	**Risorse Umane**	Il responsabile della CIE		
29	**Risorse Umane**	Lo/gli incaricato/i dell'effettuazione della richiesta di CIE		
31	**Risorse Umane**	Il call center CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Acquisizione delle CIE inizializzate**		***2) Il Comune riceve dalla Prefettura un lotto di CIE, di cui ha fatto precedentemente richiesta: processo elementare di comunicazione.***
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
21	**Informazioni**	Il numero di CIE richieste		
22	**Informazioni**	Gli atti di nomina del responsabile della presa in carico delle CIE.		
23	**Reti**	-		
24	**Infrastrutture…**	Le strutture organizzative adibite alla presa in carico delle CIE ed all'eventuale trasporto verso la sede idonea alla loro conservazione		
25	**Hardware**	Nessuno		
26	**Software**	Nessuno		
27	**Risorse Umane**	Il Sindaco		
28	**Risorse Umane**	Il responsabile della CIE		
29	**Risorse Umane**	Lo/gli incaricato/i della presa in carico delle CIE		
31	**Risorse Umane**	Il call center CIE		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Acquisizione delle CIE inizializzate**		**3) Il Comune deposita le CIE ricevute dalla Prefettura presso una sede idonea al deposito di carte valori: processo elementare di elaborazione**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
21	**Informazioni**	Il numero di CIE depositate		
22	**Informazioni**	Gli atti di nomina dei responsabili del deposito delle CIE e della gestione del sito in cui sono depositate le CIE		
23	**Reti**	-		
24	**Infrastrutture…**	Le strutture organizzative adibite alla presa in carico delle CIE presso il deposito ed all'eventuale trasporto al deposito stesso		
25	**Hardware**	Nessuno		
26	**Software**	Nessuno		
27	**Risorse Umane**	Il Sindaco		
28	**Risorse Umane**	Il responsabile della CIE		
29	**Risorse Umane**	Lo/gli incaricato/i della presa in carico delle CIE		
30	**Risorse Umane**	Lo/gli incaricato/i del deposito delle CIE		
31	**Risorse Umane**	Il call center CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Rilascio CIE ai cittadini**		**1) Acquisizione quantità di sicurezza per il punto di Back office di collegamento ai servizi di emissione CIE: processo elementare di elaborazione.**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Quantità di sicurezza		
2	**Informazioni**	I rapporti di consegna (e presa in carico).		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati.		
4	**Infrastrutture…**	La sede deposito delle quantità di sicurezza		
5	**Infrastrutture…**	La sede di rilascio delle quantità di sicurezza.		
6	**Infrastrutture…**	Le strutture utilizzate per il trasporto delle quantità di sicurezza tra le due sedi.		
7	**Hardware**	Nessuno		
8	**Software**	Nessuno		
9	**Risorse Umane**	Il Sindaco		
10	**Risorse Umane**	Il responsabile CIE		
11	**Risorse Umane**	Lo/gli incaricato/i del deposito e del prelievo e consegna delle quantità di sicurezza		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Rilascio CIE ai cittadini**		**2) Approvvigionamento CIE per il punto di back office di allestimento CIE**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Le CIE richieste		
2	**Informazioni**	I rapporti di consegna (e presa in carico) delle CIE		
3	**Reti**	-		
4	**Infrastrutture…**	La sede di deposito delle CIE		
5	**Infrastrutture…**	La sede di rilascio delle CIE ai cittadini		
6	**Infrastrutture…**	Le strutture utilizzate per il trasporto delle CIE tra le due sedi		
7	**Hardware**	Nessuno		
8	**Software**	Nessuno		
9	**Risorse Umane**	Il Sindaco		
10	**Risorse Umane**	Il responsabile CIE		
11	**Risorse Umane**	Lo/gli incaricato/i del deposito e del rilascio delle CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Rilascio CIE ai cittadini		3) Acquisizione dei dati dai cittadini
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
12	**Informazioni**	Archivio anagrafico del Comune		
13	**Informazioni**	Archivio delle abilitazioni per l'accesso ai dati anagrafici		
14	**Informazioni**	I dati anagrafici e biometrici dei cittadini		
15	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
16	**Infrastrutture…**	Il sistema informativo comunale		
17	**Infrastrutture…**	La sede presso cui si acquisiscono i dati anagrafici dei cittadini		
18	**Hardware**	I sistemi informatici del Comune		
19	**Hardware**	il punto di front office di acquisizione dei dati ed i relativi apparati per l'acquisizione dei dati anagrafici e biometrici dei cittadini.		
20	**Hardware**	Il punto di Back office per l'allestimento delle CIE.		
22	**Software**	La procedura software di acquisizione dei dati anagrafici e biometrici installata sulla postazione di front office di acquisizione dati.		
23	**Software**	La procedura software per l'integrazione con l'anagrafe comunale, installata sulla postazione di front office di acquisizione dati.		
25	**Risorse Umane**	Il responsabile dei sistemi informatici del Comune		
26	**Risorse Umane**	Il responsabile dell'anagrafe		
27	**Risorse Umane**	Il responsabile della CIE		
28	**Risorse Umane**	L'operatore incaricato del rilascio CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		**Rilascio CIE ai cittadini**		**4) Invio della richiesta di emissione ad SSCE**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Richiesta di emissione		
2	**Informazioni**	Ricevuta della richiesta di emissione		
3	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
4	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
5	**Infrastrutture…**	La/e sede/i presso cui sono installate le postazioni di back office di allestimento della CIE		
6	**Infrastrutture…**	La sede presso cui è installata la postazione di back office per la comunicazione ai servizi di emissione CIE		
7	**Infrastrutture…**	La sede presso cui è installata la Porta di accesso ai domini applicativi del CNSD		
8	**Hardware**	Hardware del punto di back office di allestimento della CIE.		
9	**Hardware**	Hardware del punto di back office per la comunicazione ai servizi di emissione CIE.		
10	**Hardware**	Hardware della Porta di accesso ai domini applicativi del CNSD		
11	**Software**	La procedura software di invio delle richieste ad SSCE, presente sul punto di back office di allestimento della CIE.		
12	**Software**	La procedura software presente sul punto di back office di comunicazione con i servizi SSCE.		
14	**Risorse Umane**	Il responsabile della CIE		
15	**Risorse Umane**	L'operatore incaricato dell'invio delle richieste di emissione CIE tramite una postazione di emissione		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Rilascio CIE ai cittadini**		**5) Ricezione, da servizi di emissione CIE, degli elementi necessari al rilascio**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Autorizzazione all'emissione		
2	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
3	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
4	**Infrastrutture…**	La sede presso cui è presente il punto di back office di allestimento della CIE		
5	**Infrastrutture…**	La sede presso cui è presente il punto di back office per la comunicazione ai servizi di emissione CIE		
6	**Infrastrutture…**	La sede presso cui è presente la Porta di accesso ai domini applicativi del CNSD		
7	**Hardware**	Hardware del punto di back office di allestimento della CIE.		
8	**Hardware**	Hardware del punto di back office per la comunicazione ai servizi di emissione CIE.		
9	**Hardware**	Hardware della Porta di accesso ai domini applicativi del CNSD.		
10	**Software**	La procedura software di invio delle richieste ad SSCE, presente sul punto di back office di allestimento della CIE.		
11	**Software**	La procedura software presente sul punto di back office di comunicazione con i servizi SSCE.		
13	**Risorse Umane**	Il responsabile della CIE		
14	**Risorse Umane**	l'operatore incaricato della ricezione delle autorizzazioni all'emissione CIE		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Rilascio CIE ai cittadini**		**6) Lavorazione elettronica e grafica delle CIE**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
44	**Informazioni**	Autorizzazioni all'emissione		
45	**Informazioni**	Dati anagrafici e biometrici dei cittadini		
46	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
47	**Informazioni**	CIE stampate correttamente		
48	**Informazioni**	CIE non stampate correttamente		
49	**Informazioni**	Report sulle operazioni di stampa concluse correttamente		
50	**Informazioni**	Report sulle operazioni di stampa non concluse correttamente		
51	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
52	**Infrastrutture…**	La sede presso cui è presente la postazione di back office per l'allestimento delle CIE che esegue la lavorazione elettronica e grafica delle CIE.		
53	**Hardware**	Hardware della postazione di back office per l'allestimento delle CIE che esegue la lavorazione elettronica e grafica delle CIE.		
54	**Software**	La procedura software che gestisce la lavorazione elettronica e grafica delle CIE, presente sulla postazione di back office per l'allestimento delle CIE		
55	**Risorse Umane**	Il responsabile della CIE		
56	**Risorse Umane**	L'operatore incaricato della lavorazione elettronica e grafica delle CIE		

MACROPROCESSO		**PROCESSO**		**ATTIVITÀ**
Emissione CIE		**Rilascio CIE ai cittadini**		**7) Attivazione CIE e rilascio ai cittadini**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
57	**Informazioni**	Archivio delle abilitazioni per l'uso dei sistemi comunali		
58	**Informazioni**	CIE stampate correttamente		
59	**Informazioni**	Report sulle operazioni di attivazione e consegna CIE concluse regolarmente		
60	**Informazioni**	Report sulle operazioni di attivazione e consegna CIE non concluse regolarmente		
61	**Informazioni**	Dati anagrafici dei cittadini per la loro identificazione in fase di consegna delle CIE personalizzate		
62	**Reti**	Le reti dati del Comune sulle quali transitano gli asset informativi individuati		
63	**Reti**	Le reti dati del Comune verso la porta di accesso ai servizi del CNSD e, attraverso questa, ai servizi di convalida anagrafica del CNSD, ai servizi di verifica validità del certificato CIE del SSCE, ai servizi di attivazione CIE del SSCE		
64	**Infrastrutture…**	Le sedi presso cui sono presenti i punti di front office di rilascio e attivazione della CIE		
65	**Hardware**	Hardware del punto di front office di rilascio e attivazione CIE.		
66	**Software**	La procedura software che gestisce l'attivazione delle CIE, presente sul punto di front office di rilascio e attivazione CIE.		
67	**Risorse Umane**	Il responsabile della CIE		
68	**Risorse Umane**	L'operatore incaricato dell'attivazione e consegna delle CIE ai cittadini		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Rilascio CIE ai cittadini		8) Riconsegna CIE a deposito processo elementare di comunicazione. Lo/gli incaricato/i della riconsegna delle CIE riporta le CIE non utilizzate alLo/agli incaricato/i del deposito delle CIE (idoneo alle carte valori).
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
69	Informazioni	Le CIE non utilizzate		
70	Informazioni	Le CIE non stampate correttamente		
71	Informazioni	Le CIE non consegnate per indisponibilità del cittadino		
72	Informazioni	I rapporti di consegna (e presa in carico) delle CIE		
73	Informazioni	Gli atti ed i documenti di autorizzazione al deposito o alla consegna CIE		
74	Reti	-		
75	Infrastrutture …	La sede deposito delle CIE		
76	Infrastrutture …	La/e sede/i di rilascio delle CIE ai cittadini		
78	Hardware	Nessuno		
79	Software	Nessuno		
80	Risorse Umane	Il Sindaco		
81	Risorse Umane	Il responsabile CIE		
82	Risorse Umane	Gli incaricati del deposito e della riconsegna delle CIE		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Emissione CIE		Rilascio CIE ai cittadini		**9) Riconsegna quantità di sicurezza**
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Le quantità di sicurezza		
2	**Informazioni**	I relativi rapporti di consegna (e presa in carico)		
3	**Informazioni**	Gli atti ed i documenti di autorizzazione al deposito o alla consegna delle quantità di sicurezza		
4	**Reti**	-		
5	**Infrastrutture …**	La sede deposito delle quantità di sicurezza		
6	**Infrastrutture …**	La sede del punto di back office per la comunicazione con i servizi di emissione CIE.		
8	**Hardware**	Nessuno		
9	**Software**	Nessuno		
10	**Risorse Umane**	Il Sindaco		
11	**Risorse Umane**	Il responsabile CIE		
12	**Risorse Umane**	Lo/gli incaricato/i del deposito e della riconsegna delle quantità di sicurezza		

MACROPROCESSO		PROCESSO		ATTIVITÀ
Uso della CIE		Abilitazione di un server comunale per l'identificazione in rete dei cittadini che accedono tramite CIE ai servizi in rete del Comune		1) Abilitazione di un server comunale per l'identificazione in rete dei cittadini che accedono tramite CIE ai servizi in rete del Comune
ID	**Classi**	**Asset**	**Minacce**	**Vulnerabilità**
1	**Informazioni**	Il sito web del Comune per il riconoscimento tramite CIE		
2	**Informazioni**	Le indicazioni del Ministero dell'Interno sulle modalità di accesso ai servizi distribuiti per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE		
2	**Informazioni**	L'autorizzazione del Ministero dell'Interno all'accesso ai servizi distribuiti del CNSD per la verifica della validità dei certificati di sicurezza e delle informazioni anagrafiche memorizzati sulle CIE		
2	**Informazioni**	Il servizio CNSD di convalida INA		
6	**Reti**	Le reti di comunicazione verso la Porta di accesso ai domini applicativi del CNSD		
6	**Reti**	Le reti di comunicazione tra la Porta di accesso ai domini applicativi del CNSD ed il CNSD stesso		
7	**Infrastrutture…**	Le strutture organizzative utilizzate per la realizzazione dei software utilizzati a livello del server comunale		
9	**Hardware**	I sistemi che ospitano il WEB server del Comune		
9	**Hardware**	La porta comunale di accesso ai domini applicativi del CNSD		
10	**Software**	Il WEB server del Comune		
13	**Risorse Umane**	Il Sindaco		
14	**Risorse Umane**	Il responsabile CIE		
14	**Risorse Umane**	Le strutture organizzative che hanno realizzato le applicazioni informatiche per accedere ai servizi del CNSD.		
16	**Risorse Umane**	Gli operatori incaricati della gestione del sito web comunale		

3. Minacce e vulnerabilità

3.1. Minacce

Una minaccia è la causa potenziale di un evento non desiderato che può avere come conseguenza danni al Comune ed ai suoi asset.

Gli eventi possono essere:
- naturali (esondazione, terremoto, …)
- intenzionali
- accidentali.

In genere, l'evento, cioè l'attuarsi di una minaccia, può consistere in:

- distruzione di un asset
- corruzione o modifica di un asset
- sottrazione o perdita di un asset
- pubblicazione di informazioni riservate
- uso non lecito di un asset
- interruzione del servizio

Di seguito si riporta una lista delle più frequenti minacce e delle conseguenze negative che esse potrebbero provocare sulla riservatezza, integrità, disponibilità, responsabilità, autenticità ed affidabilità delle informazioni.

In relazione alle minacce ed alla loro potenziale incidenza sulla sicurezza dell'informazione, il Comune deve:
- identificare ed eventualmente aggiungere nuove minacce relative al proprio contesto operativo
- valutare quali aspetti relativi alla sicurezza dell'informazione, possono essere influenzati da tali minacce (riservatezza, integrità, disponibilità, responsabilità, autenticità ed affidabilità delle informazioni)

TABELLA – INCIDENZA DELLE MINACCE SULLE INFORMAZIONI

Id	Minaccia	Riservatezza	Integrità	Disponibilità	Responsabilità	Autenticità	Affidabilità
Minacce Ambientali							
1	Contaminazione			✓			
2	Terremoto			✓			
3	Interferenze Elettroniche			✓			
4	Valori estremi di temperatura e umidità			✓			
5	Blackout			✓			
6	Incendio			✓			
7	Esondazione/Inondazione			✓			
8	Fluttuazioni dell'alimentazione elettrica			✓			
9	Tempesta			✓			
10	Cambiamenti della marea			✓			
11	Parassiti			✓			
Minacce Intenzionali							
12	Denial of Service (attacchi informatici che causano la disconnessione dal server o il possibile blocco del computer.)			✓			
13	Appropriazione indebita di informazioni protette	✓					

14	Incendio			✓			
15	Attività industriali			✓			
16	Codice dannoso (virus, …)	✓	✓	✓			
17	Distruzione intenzionale dei dati e delle strutture		✓	✓	✓		✓
18	IP Masquerading (attacco informatico che comporta la falsificazione degli indirizzi IP con conseguente falsificazione del mittente reale della comunicazione)	✓	✓		✓	✓	
19	Ripudio delle comunicazioni o transazioni compiute				✓	✓	
20	Sabotaggio		✓	✓			
21	Induzione fraudolenta a rivelare o diffondere dati sensibili (in particolar modo su Internet)	✓	✓	✓	✓	✓	
22	Furto e frode	✓		✓	✓	✓	
23	Accesso non autorizzato ai dati	✓	✓		✓	✓	✓
24	Accesso non autorizzato a un server di posta	✓	✓		✓	✓	✓
25	Cambiamenti di software non autorizzati	✓	✓	✓	✓		✓
26	Uso di "software pirata" (software privo di relativa licenza e scaricato, per esempio, da internet con i relativi aggiornamenti)			✓	✓		✓
27	Intrusione di "hacker" in siti web (attacchi informatici effettuati verso i siti web con relativa alterazione degli stessi)	✓	✓	✓		✓	
Minacce Accidentali							
28	Incendio dell'edificio			✓			

29	Guasto degli apparati di comunicazione			✓			
30	Errori imputabili a terzi, in servizi gestiti in outsourcing (ovvero gestiti da personale esterno all'amministrazione comunale)	✓	✓	✓			
31	Assenza di personale "chiave" ovvero di personale indispensabile per la corretta erogazione dei servizi	✓	✓	✓			✓
32	Invio dei messaggi su canali di comunicazione non adatti o non errati (esempio: invio di fax al numero sbagliato)	✓	✓	✓			
33	Errori del Personale Operativo		✓	✓			
34	Errori imputabili al software	✓	✓	✓			✓
35	Guasti tecnici		✓	✓			✓
36	Errori delle linee di trasmissione dati		✓	✓			✓

3.2. Vulnerabilità

Le vulnerabilità sono i punti deboli degli asset individuati.
Una vulnerabilità è un insieme di condizioni che possono consentire ad una minaccia di influire su un asset.

Tipicamente una vulnerabilità è conseguenza di:
- un'errata procedura (informatica e/o organizzativa),
- personale non sufficientemente addestrato,
- tecnologie non correttamente configurate,
- tecnologie difettose.

La conoscenza dello stato reale di un sistema di servizi, nel contesto della sicurezza, ovvero la consapevolezza delle vulnerabilità esistenti, consente di orientare i comportamenti all'interno dell'organizzazione in modo tale da ridurre, nella misura massima possibile, il pericolo che gli eventi temuti possano verificarsi.

D'altra parte, ove i punti deboli del sistema vengano conosciuti all'esterno dell'organizzazione, aumenta la probabilità che eventi lesivi intenzionali possano concretamente verificarsi.

Il Comune, nell'apposita scheda "*Classificazione delle minacce e delle vulnerabilità*", è tenuto ad individuare per ciascuna minaccia associata agli asset, tutte le vulnerabilità presenti nella propria realtà organizzativa, logistica e tecnica ed a specificare, negli appositi campi, su quali aspetti della sicurezza dell'informazione, dette minacce vanno ad incidere.

Il formato delle schede da utilizzare in questa fase è riportato di seguito.

CLASSIFICAZIONE DELLE MINACCE E DELLE VULNERABILITA'

Campo	**Descrizione**
R	Riservatezza
I	Integrità
D	Disponibilità
Re	Responsabilità
Au	Autenticità
Af	Affidabilità

Id - asset	Minaccia	R	I	D	Re	Au	Af	Elenco Vulnerabilità

La rilevazione delle vulnerabilità rispetto alle minacce consente:

- la misurazione del livello di pericolosità di una minaccia rispetto al sistema comunale;
- la classificazione esaustiva delle minacce da considerare nel piano
- l'analisi e la rilevazione nella seconda fase di redazione del piano di sicurezza di nuove vulnerabilità e, conseguentemente delle potenziali minacce ad esse associate non considerate nella versione precedente del piano(alfa). Tali minacce dovranno essere indicate negli appositi modelli in aggiunta a quelle già in precedenza inserite.

È appena il caso di sottolineare che esistono minacce rilevanti per la realtà comunale non necessariamente associate a specifiche vulnerabilità: queste minacce possono essere inserite nel piano di sicurezza anche se non collegate a vulnerabilità specificamente individuate.
Si rileva al contrario che una minaccia per la quale siano state rilevate una o più vulnerabilità, deve essere obbligatoriamente inserita nel piano di sicurezza.

Di seguito si riporta un elenco esemplificativo delle vulnerabilità più diffuse.

1) Presenza di materiali infiammabili quali carta o scatoloni
2) Archivi e Sistemi di back-up non disponibili
3) Interfacce complesse delle applicazioni software
4) Pagine WEB che presentano informazioni che possono esporre l'organizzazione ad accessi non autorizzati
5) Malfunzionamenti nei processi organizzativi di cambiamento dell'amministrazione
6) Cablaggio (cavi e linee di rete) inadeguato
7) Manutenzione impropria o inappropriata delle apparecchiature tecniche
8) Controllo inadeguato della distribuzione del software
9) Formazione inadeguata del personale relativamente al problema dei virus informatici
10) Regole inadeguate sui firewall e sugli apparati per la sicurezza delle reti
11) Gestione inadeguata degli incidenti di sicurezza
12) Politiche inadeguate sulla sicurezza delle informazioni
13) Monitoraggio inadeguato delle condizioni ambientali
14) Gestione della rete inadeguata
15) Report inadeguati sul malfunzionamenti delle applicazioni informatiche
16) Insufficiente separazione delle funzioni tra personale tecnico e personale amministrativo
17) Standard inadeguati per le attività di sviluppo delle applicazioni software
18) Controllo inadeguato dei gruppi di sviluppo del software
19) Privilegi di accesso errati ai sistemi informatici comunali
20) Applicazioni di controllo della sicurezza non correttamente configurate o non adeguate allo stato dell'arte
21) Sistemi operativi non correttamente configurati o aggiornati
22) Insufficiente formazione sulla sicurezza
23) Mancanza di sistemi di sicurezza sulle reti (firewall, proxy, …)
24) Mancanza di un inventario delle linee dial-up (connessioni remote) che comportano l'impossibilità di conoscere la quantità e la frequenza degli accessi dial-up ai sistemi comunali
25) Mancanza di sistemi che rilevino, in tempo reale, eventi su rete non autorizzati
26) Mancanza di un sistema antincendio automatico
27) Mancanza di dispositivi o procedure di back-up
28) Mancanza di dispositivi per la rilevazione di incendi
29) Carente manutenzione degli impianti e dei dispositivi
30) Basso livello di affidabilità delle reti di comunicazione a causa di manutenzione o progettazione impropria
31) Apparecchiature tecniche non sufficientemente protette
32) Inesistenza di sistemi di backup per i sistemi server critici del Comune
33) Mancanza di aggiornamenti regolari del software antivirus
34) Mancanza di aggiornamenti di sicurezza del sistema operativo
35) Il Sistema è localizzato in un'area suscettibile alle fluttuazioni di energia elettrica

4.Valutazione del rischio

Come già accennato nel precedente capitolo, la valutazione del rischio è effettuata in base all'incidenza delle minacce.

Il formato delle schede da utilizzare in questa fase è riportato di seguito.

TABELLA DI VALUTAZIONE DEL RISCHIO

Impatto	
Campo	**Descrizione**
R	Riservatezza
I	Integrità
D	Disponibilità
Re	Responsabilità
Au	Autenticità
Af	Affidabilità

Valore		
Sigla	**Descrizione**	**Peso**
N	Nullo	0
B	Basso	1
M	Medio	3
A	Alto	7
C	Critico	15

MACROPROCESSO Titolo del Macroprocesso							PROCESSO Titolo del processo	ATTIVITÀ Descrizione dell'attività		
Minaccia	Impatto						Rischio			
	R	I	D	Re	Au	Af	Valore (NBMAC)	Provoca interruzione del servizio? (Si/No)	Commento

4.1. Modalità di compilazione ed uso della tabella di valutazione del rischio

In analogia con le "Schede di Classificazione delle minacce e delle vulnerabilità", la tabella precedente va compilata per ogni macroprocesso, processo e attività elementare, specificando la denominazione del macroprocesso, del processo e dell'attività. Gli ulteriori elementi che devono essere specificati, sono di seguito elencati e descritti:

- Minacce: il compilatore deve riportare nelle apposite caselle, tutte le minacce elencate nelle "Schede di Classificazione delle minacce e delle vulnerabilità".
- Impatto: le sei colonne corrispondono a R-Riservatezza, I-Integrità, D-Disponibilità, Re-Responsabilità, Au-Autenticità, Af-Affidabilità.

- Indicare, per ogni singola minaccia, l'impatto della minaccia sul processo elementare considerato. I valori sono: N-Nullo, B-Basso, M-Medio, A-Alto, C-Critico. Utilizzare la tabella "Tabella – incidenza delle minacce sulle informazioni" ed associare un valore di impatto (N,B,M,A,C).
- Rischio: il valore di rischio corrisponde alla media dei valori numerici associati alle singole voci di impatto. I valori da utilizzare in questo piano (alfa) sono i seguenti:
  - N-NULLO = 0
  - B-BASSO = 1
  - M-MEDIO = 3
  - A-ALTO = 7
  - C-CRITICO = 15
- Per ogni riga e per ogni elemento R-Riservatezza, I-Integrità, D-Disponibilità, Re-Responsabilità, Au-Autenticità, Af-Affidabilità, si sommano tali valori e si calcola la media finale.
  - A titolo di esempio, supponiamo che per la minaccia "Accesso Non autorizzato ai Dati", il Comune, nelle colonne indicate dalla tabella "Incidenza Delle Minacce Sulle Informazioni", abbia inserito i valori che seguono:

		R	I	D	Re	Au	Af
	Accesso Non autorizzato ai Dati	A	C	N	B	B	M

- Ora, sommando i valori accoppiati ad
  A-C-N-B-B-M, cioè: 7+15+1+1+3, si ottiene 27. Si divide per 6 e si ottiene 27/6=4,5 che si arrotonda al valore immediatamente più alto, quindi a 5.

- Si noti come l'impatto sulla disponibilità sia stato messo a N-NULLO in quanto la colonna "Disponibilità" nella tabella "INCIDENZA DELLE MINACCE SULLE INFORMAZIONI" non è marcata per questo tipo di minaccia.

- Per la colonna del rischio, si utilizza poi la seguente regola di trasformazione
  - 0 ➔ N-NULLO
  - 1 ➔ B-BASSO
  - 2|3|4 ➔ M-MEDIO
  - 5|6|7|8|9 ➔ A-ALTO
  - 10|11|12|13|14|15 ➔ C-CRITICO
- Il corrispondente di 5, quindi come valore da inserire nella colonna del rischio, è A-ALTO.

- Provoca interruzione del servizio? (Sì/No)
  - Indica se l'avverarsi della minaccia provoca l'interruzione del servizio relativo al macroprocesso, processo ed attività/processo elementare.

- Commento: casella a disposizione del responsabile della sicurezza CIE per indicare elementi ulteriori da utilizzare nella successiva fase di trattamento del rischio.

5. Trattamento del rischio

La tabella di trattamento del rischio va compilata per tutti i rischi che si intendono trattare.
La tabella di trattamento del rischio prevede in particolare una colonna nella quale il responsabile della sicurezza CIE deve descrivere in che modo assicura l'attuazione dei controlli richiesti per ogni macroprocesso, processo e processo elementare indicati nell'allegato 3.

TABELLA TRATTAMENTO RISCHIO

MACROPROCESSO Titolo del Macroprocesso				PROCESSO Titolo del processo	ATTIVITÀ Descrizione dell'attività		
Minaccia	Trattamento scelto	Politiche di sicurezza di riferimento per il trattamento scelto	Responsabile	Risorse	Tempi	È garantita la continuità del servizio? (Sì/No)	Controlli

Nel piano alfa, si devono considerare le sole minacce alle quali corrisponda uno dei seguenti valori di rischio:
- CRITICO,
- ALTO,
- MEDIO.

Nel caso in cui il Comune non intenda risolvere una particolare minaccia, deve specificare i motivi del mancato trattamento, motivi che possono essere di natura economica (troppo elevato il costo di trattamento della minaccia), statistica (la minaccia è estremamente improbabile) o organizzativa (l'organizzazione comunale già gestisce il particolare tipo di minaccia in un contesto esterno al progetto CIE).

Le minacce il cui valore di rischio è corrispondente a "BASSO", devono comunque essere tenute sotto controllo, quindi non è necessario che il Comune ponga in essere attività per neutralizzarle, ma è sufficiente che le stesse siano costantemente monitorate e controllate.

Di seguito si riporta la descrizione della scheda:

- Minaccia: la minaccia, così come individuata nelle tabelle di analisi del rischio.
- Trattamento scelto: le azioni che si intendono intraprendere per attenuare/risolvere prevenire e/o tenere sotto controllo la minaccia, ovvero, il nome del documento che descrive il trattamento che si intende attuare, in caso di procedura molto articolata. La stessa procedura può afferire a più minacce.
  Inoltre, nel caso in cui si preveda di aggiornare il trattamento, devono essere definiti:
  - Politiche di sicurezza di riferimento per il trattamento scelto: elenco delle politiche di sicurezza che sono state prese in considerazione per il trattamento stesso.
  - Responsabile: specificare il nominativo del responsabile del trattamento specificandone il ruolo professionale che riveste all'interno dell'organizzazione.
  - Risorse: le risorse (personale, infrastrutture, logistiche, sistemi di elaborazione, etc.) dedicate a tale trattamento.
  - Tempi: riportare una stima dei tempi (giorni solari) pianificati per l'attuazione del trattamento scelto.

- È garantita la continuità del servizio? (Sì/No): il responsabile della sicurezza CIE deve indicare se il trattamento indicato sia idoneo ad evitare il verificarsi dell'evento temuto (interruzione del servizio).

- Controlli: nella casella corrispondente, va specificata la tipologia di controllo, tra quelli indicati nell'allegato 3 in corrispondenza dei processi elementari, che viene assicurata dal trattamento prescelto.
  In particolare le attività di controllo, di cui all'allegato 3, possono essere previste sia nelle procedure operative del piano di sicurezza comunale, sia nell'ambito delle procedure di trattamento dei rischi e delle minacce.

  Il Comune è tenuto alla redazione della scheda sotto riportata.

CORRISPONDENZA DEI CONTROLLI OBBLIGATORI

MACRO PROCESSO	PROCESSO	ATTIVITÀ	CONTROLLI OBBLIGATORI	CORRISPONDENZA NEL PIANO DI SICUREZZA CIE

6. Attuazione dei trattamenti

La fase DO della metodologia di realizzazione e gestione del piano della sicurezza dei Comuni CIE prevede la trasformazione delle tabelle di trattamento del rischio (cap. 5) nel diagramma GANTT del piano di sicurezza Comunale.

La fase di trasformazione è immediata: è necessario aggiungere alle tabelle di trattamento del rischio, di cui al capitolo 5, le date di inizio e termine delle attività.
La tabella di trattamento del rischio si trasforma in:

ATTUAZIONE DEGLI INTERVENTI

MACROPROCESSO Titolo del Macroprocesso		PROCESSO Titolo del processo		ATTIVITÀ Descrizione dell'attività	
Minaccia	Trattamento scelto	Responsabile	Data inizio trattamento	Data fine trattamento	Risorse

Il Comune può ora, sulla base del diagramma GANTT, procedere all'attuazione del piano di sicurezza.
Dal punto di vista metodologico, inizia ora la fase CHECK, che ha l'obiettivo di monitorare e validare l'attuazione del piano di sicurezza.

7. Definizione delle procedure operative

Il Comune deve elaborare le procedure operative relative al piano di sicurezza, tenendo conto della propria struttura tecnica ed organizzativa.
Le procedure operative per la sicurezza dovranno pertanto essere definite sia sulla base delle procedure amministrative/organizzative esistenti, sia in relazione ai trattamenti individuati.
La stessa procedura operativa può essere riferita ad un pluralità di trattamenti.

7.1. Modulo di definizione e descrizione delle procedure operative

Partendo dai trattamenti individuati, per la redazione delle procedure operative il Comune deve definire e descrivere la procedura utilizzando il modulo qui indicato.
Nei paragrafi seguenti si riporta:

- modulo di definizione e descrizione delle procedure operative;
- elenco delle procedure operative "obbligatorie", ovvero delle procedure operative considerate indispensabili per la gestione della sicurezza.

MODULO PROCEDURA OPERATIVA

<table>
<tr><td colspan="2">Procedura</td><td colspan="4"></td></tr>
<tr><td colspan="2">Descrizione sintetica della procedura</td><td colspan="4"></td></tr>
<tr><td colspan="2">Macroprocessi o processi nell'ambito delle attività di emissione ed uso CIE</td><td colspan="4"></td></tr>
<tr><td colspan="2">Politiche di sicurezza di riferimento</td><td colspan="4"></td></tr>
<tr><td colspan="6">Descrizione Ruoli e Competenze</td></tr>
<tr><td colspan="2">Ruolo</td><td colspan="4">Descrizione delle Competenze</td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="6">Descrizione delle Risorse</td></tr>
<tr><td>Tipologia</td><td>Risorsa</td><td>Funzionalità</td><td>Responsabile</td><td>Gestione degli accessi</td><td>Controlli</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Descrizione del flusso della procedura</td></tr>
<tr><td colspan="6"></td></tr>
</table>

Per la compilazione della tabella, si forniscono le seguenti indicazioni.:

- *Descrizione sintetica della procedura*: Occorre evidenziare gli aspetti più importanti ai fini della sicurezza.
- *Ruolo*: In considerazione dei ruoli professionali già descritti in precedenza nell'ambito della descrizione della struttura comunale, elencare i soli ruoli di interesse per la procedura.
- *Descrizione delle competenze*: indicazione delle competenze afferenti al ruolo professionale.
- *Tipologia*: Riportare la tipologia della risorsa in base alla seguente classificazione:
    - Risorsa tecnologica:
        - risorse di rete
        - Porta di accesso ai domini applicativi del CNSD
        - Postazioni di emissione
        - Postazioni di Lavoro
        - Postazioni server
        - Altre risorse tecnologiche
    - Risorsa logistica:
        - ambienti
        - chiavi di accesso fisico
    - Risorsa informativa:
        - registri (sia cartacei che informatici)
        - basi dati
        - autorizzazioni all'accesso ai sistemi ed alle risorse informatiche
        - altre risorse informative
- *Funzionalità*: la funzione svolta dalla risorsa all'interno della procedura.
- *Gestione degli accessi*: Descrivere le modalità di gestione degli accessi alla risorsa con riferimento alla procedura;
- *Descrizione del flusso della procedura*: descrivere il flusso di lavoro della procedura, indicando i momenti di interazione tra le diverse figure professionali coinvolte.

7.2. Procedure operative obbligatorie

In riferimento alle politiche di sicurezza indicate ed ai Macroprocessi di emissione ed uso della CIE precedentemente descritti, ai fini della sicurezza è obbligatorio che i Comuni definiscano le seguente procedure operative:

- *Procedura di controllo degli accessi*. Comprende:
    - La gestione degli accessi ai luoghi dove sono installate le postazioni di front office e back office per l'emissione delle CIE.
    - Le modalità di concessione e revoca delle autorizzazioni di accesso.
    - Le modalità di registrazione degli accessi.
    - I controlli previsti.
- *Procedura di gestione degli account*. Disciplina:
    - Gli accessi a tutti gli apparti inerenti la sicurezza dei processi di emissione ed uso della CIE,
    - Le modalità di attribuzione e distribuzione delle password,
    - Le modalità di definizione, aggiornamento e revoca degli account.

- *Procedura di registrazione dei sistemi comunali presso la Porta di Accesso ai domini applicativi del CNSD*.
- *Procedura di gestione del materiale in entrata ed in uscita*:
  - Disciplina i flussi in entrata ed in uscita dei materiali, nonché la regolare consenga al responsabile.
- *Procedura di gestione delle Quantità di Sicurezza*.
  - Disciplina l'acquisizione della quantità di sicurezza e la relativa custodia.
- *Procedura di gestione delle CIE inizializzate*:
  - Disciplina, all'interno del Comune, le attività di richiesta e custodia delle CIE inizializzate.
  - Disciplina la presa in carico da parte dei responsabili delle postazioni di emissione, la riconsegna delle carte non stampate, l'accantonamento delle carte non utilizzabili.
- *Procedura di Manutenzione degli apparati*:
  - Disciplina gli interventi di manutenzione ordinaria (controllo dei virus, aggiornamenti software, etc.) e straordinaria (per guasti hardware, per malfunzionamenti software, etc.).
- *Procedura di Gestione della rete*
- *Procedura di Gestione della Porta di accesso ai domini applicativi del CNSD*:
  - Disciplina gli accessi (concessione/revoca), gli interventi (manutenzione, aggiornamento), l'uso della porta di accesso ai domini applicativi del CNSD.
- *Procedura di Gestione delle Postazioni di Emissione*:
  - Disciplina gli accessi (concessione/revoca), gli interventi (manutenzione, aggiornamento), l'uso delle postazioni di emissione di front office e/o back office.
- *Procedura di emissione CIE*:
  - Complesso delle regole e delle descrizione del modello organizzativo di riferimento per l'emissione CIE evidenziando tutte le regole di sicurezza prevista
- *Procedura di caricamento dell'INA*
- *Procedure di attuazione delle norme vigenti inerenti la sicurezza dell'edificio e del personale*
- *Procedure operative per la gestione di eventi straordinari*: descrizione della modalità di gestione dei backup e dei possibili livelli di eventuali eventi straordinari.

Le procedure obbligatorie, qualora richiesto possono essere suddivisi in più sottoprocedure.

Allegato 5
MONITORAGGIO E VALIDAZIONE DEL PIANO

1. Introduzione

La fase di CHECK (monitoraggio e validazione) della metodologia prevede che, a partire dal diagramma GANTT elaborato nella precedente fase DO, venga verificata dal responsabile CIE, la corretta attuazione del piano di lavoro.

2. Schede di attuazione, monitoraggio e validazione del piano di sicurezza

Le schede di attuazione e monitoraggio del Piano di sicurezza consentono sia di controllare lo stato di attuazione del Piano di sicurezza comunale CIE, sia di monitorare tutti gli eventi di interesse per la sicurezza comunale CIE.
Il Comune è quindi tenuto ad inviare le schede compilate alla Prefettura.
Il responsabile comunale della sicurezza CIE è tenuto a redigere tali schede con frequenza trimestrale dalla data di approvazione del Piano di sicurezza da parte della Prefettura.

2.1. Schede di attuazione

Rispetto al modulo qui presentato, il Comune, con riferimento al proprio piano di sicurezza comunale CIE, è tenuto ad aggiornare:

- l'elenco dei responsabili
- l'elenco delle procedure operative
- l'elenco delle minacce con i relativi trattamenti rispetto al piano di sicurezza comunale CIE.

Il modulo è stato predisposto riportando solo i responsabili e le procedure operative obbligatorie.

Stato di attuazione del Piano di sicurezza comunale CIE	
Stato di nomina responsabili	
Responsabile previsti nel Piano	*Nominato?(SI/NO)*
Responsabile comunale per la sicurezza degli accessi al CNSD	
Responsabile della sicurezza CIE	
Responsabile della custodia delle Quantità di Sicurezza	
Responsabile caricamento INA	
Responsabile di emissione CIE	
Responsabile della sicurezza dei dati	

Responsabile delle postazioni di emissione sia di front office che di back office	
Responsabile della Porta di accesso ai domini applicativi del CNSD	
Responsabile della rete	
Responsabile dei servizi tecnici	
Responsabile delle verifiche e delle ispezioni (auditing)	
Responsabile della manutenzione	

Stato Procedure Operative

Procedure operative	Attuata? (SI/NO/PARZIALMENTE)
Procedura di controllo degli accessi	
Procedura di gestione degli account	
Procedura di gestione del materiale in entrata ed in uscita	
Procedura di attivazione dei sistemi comunali	
Procedura di gestione della Quantità di Sicurezza	
Procedura di gestione delle CIE inizializzate	
Procedura di manutenzione degli apparati	
Procedura di gestione della rete	
Procedura di gestione della porta di accesso ai domini applicativi del CNSD	
Procedura di gestione delle postazioni di emissione	
Procedura di emissione CIE	
Procedura di caricamento dell'INA	
Procedure di attuazione delle norme vigenti inerenti la sicurezza dell'edificio e del personale	
Procedure di attuazione delle direttive del Ministero dell'Interno	
Procedure operative per la gestione di eventi straordinari	

Stato di attuazione dei trattamenti per le minacce

Minaccia	*Trattamento*	*Attuato? (SI/NO)*

2.2. Schede di monitoraggio e validazione

Le schede di monitoraggio e validazione vanno compilate dal Comune che, per ogni macroprocesso e processo elementare, deve considerare tutti gli avvenimenti rilevanti ai fini della sicurezza degli asset individuati nel piano.

Per gli eventi non previsti nel piano di sicurezza, il responsabile della sicurezza CIE deve comunque individuare quali attività porre in essere per risolvere l'evento di rischio.

Di seguito si riporta il modulo di monitoraggio e la tracciatura degli eventi di interesse per la sicurezza comunale CIE.

MACROPROCESSO Titolo del Macroprocesso	PROCESSO Titolo del processo	ATTIVITÀ Descrizione dell'attività
	Nuovo Processo? ☐ SI ☐ NO	Nuova Attività? ☐ SI ☐ NO

Evento	Minaccia prevista (si/no)	Minaccia e Vulnerabilità	Esito dell'intervento (Risolto/Non risolto)	Ha provocato interruzione di servizio? (Sì/No)	Descrizione delle attività condotte	Riferimento

La tabella va completata secondo le seguenti indicazioni:

- **Nuovo Processo**: riportare SI se il processo indicato non è presente nel piano di sicurezza. Riportare NO qualora il processo di riferimento sia già indicato nel Piano di sicurezza
- **Nuova attività** riportare SI se l'attività indicata non è presente nel piano di sicurezza. Riportare NO qualora l'attività di riferimento sia già trattata nel Piano di sicurezza;
- **Evento**: indica e descrive l'evento che si è verificato;
- **Minaccia prevista** (Sì/No): indica se la minaccia era stata analizzata nel piano oppure se è una minaccia non prevista;
- **Minaccia e vulnerabilità**: descrive l'evento che si è verificato e la vulnerabilità che lo ha reso possibile;
- **Riferimento**: con riferimento al piano di sicurezza, riportare la procedura operativa e/o il controllo di riferimento per l'evento rilevato.

Tutte i trattamenti previsti nel piano versione alfa che hanno consentito di risolvere un evento di sicurezza, sono considerati validati ai fini della prossima fase della metodologia: ACT, descritta nell'allegato 6.

Allegato 6
MANUTENZIONE ED EVOLUZIONE DEL PIANO

1. Descrizione delle attività

A seguito della fase di CHECK, sono stati individuati sia gli eventi non considerati nel piano di sicurezza CIE versione alfa, sia i trattamenti del rischio che sono invece stati utili e sono quindi stati validati.

In questa fase, a partire dalle schede di monitoraggio, si devono rivedere i requisiti alla base del piano di sicurezza comunale CIE, versione alfa, al fine di ottenere il nuovo piano, più preciso ed efficace del precedente, versione beta.

La redazione del nuovo piano di sicurezza, deve, in ogni caso essere effettuata con una frequenza annuale.

In questa fase il Comune è tenuto a formulare un rapporto che contenga una classificazione delle variazioni del nuovo piano di sicurezza comunale CIE rispetto al precedente, secondo i seguenti parametri:

- Variazioni della struttura organizzativa, logistica e tecnica
- Analisi e classificazione dei processi interessati
- Classificazione minacce, vulnerabilità e valutazione del rischio
- Variazioni delle procedure operative.

1.1. Variazioni della struttura organizzativa, logistica e tecnica

Di seguito si riporta la scheda che il Comune è tenuto a consegnare unitamente al nuovo Piano di sicurezza per evidenziare le variazioni rispetto al precedente piano circa la struttura organizzativa, logistica e tecnica comunale.

Variazione della struttura organizzativa logistica e tecnica		
Domande generali	*Stato variazione (SI/NO)*	*Commento*
La struttura logistica comunale CIE è variata?		
La struttura tecnica comunale CIE è variata?		
La struttura organizzativa comunale CIE è variata?		
Variazioni sui ruoli di responsabili		
Descrizione responsabile	*Variazione*	*Commento*
Responsabile comunale per la sicurezza degli accessi al CNSD		
Responsabile della sicurezza CIE		
Responsabile della custodia delle Quantità di Sicurezza		
Responsabile caricamento INA		

Responsabile di emissione CIE		
Responsabile della sicurezza dei dati		
Responsabile delle postazioni di emissione sia di front office che di back office		
Responsabile della Porta di accesso ai domini applicativi del CNSD		
Responsabile della rete		
Responsabile dei servizi tecnici		
Responsabile delle verifiche e delle ispezioni (auditing)		
Responsabile della manutenzione		

Nella casella "Variazione" deve essere riportata una delle seguenti voci:

- *N => Nuova voce non prevista nel piano di sicurezza precedente*
- *M => Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano*
- *R => Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano*

Nella casella "Commento" deve essere riportata una nota circa la causa della variazione rispetto al precedente piano di sicurezza.

1.2. Analisi e classificazione dei processi interessati

Nell'ambito delle schede di analisi e classificazione dei processi interessati, il Comune è tenuto ad evidenziare le variazioni del nuovo Piano di Sicurezza rispetto al precedente riportando:

- elenco dei nuovi processi organizzativi presenti nel progetto CIE, a seguito di variazioni normative, tecnologiche o logistiche intervenute dopo la stesura del piano di sicurezza alfa.
- Elenco delle nuove tecnologie introdotte nei processi comunali CIE che consentono di ridurre o eliminare completamente alcune classi di rischio.

Segue il modulo di riferimento.

Classificazione e/o aggiornamento del piano versione alfa – schede delle attività

MACROPROCESSO	PROCESSO indicare se questo è un nuovo processo che si aggiunge al piano alfa	ATTIVITÀ nel caso in cui il processo sia già presente nel piano alfa, indicare se questa attività si aggiunge al processo
	Nuovo Processo?	Nuova attività?

		☐ SI	☐ NO	☐ SI	☐ NO	
ID	Classi	Asset	Minacce	Vulnerabilità	Variazione*	Commento
	Informazioni					
	Reti					
	Infrastrutture…					
	Hardware					
	Software					
	Risorse Umane					

***Per la descrizione della variazione riportare le seguenti voci:**

- **N => Nuova voce non prevista nel piano di sicurezza precedente**
- **M=> Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano**
- **R=> Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano**

In riferimento al nuovo piano di sicurezza, per ogni asset e relativa minaccia e vulnerabilità, deve essere indicato nella casella "Variazione" lo stato di variazione rispetto al piano di sicurezza precedente. In particolare deve essere riportato una delle seguenti voci:

- *N => Nuova voce non prevista nel piano di sicurezza precedente*
- *M => Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano*
- *R => Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano*

Nella casella "Commento" deve essere riportata una nota circa la causa della variazione rispetto al precedente piano di sicurezza.

1.3. Classificazione minacce, vulnerabilità e valutazione del rischio

Per il nuovo piano di sicurezza, il Comune è tenuto a evidenziare le variazioni rispetto al precedente piano di sicurezza riportando la classificazione delle minacce e vulnerabilità e della valutazione del rischio. Le variazioni possono essere dovute a:

- trattamenti che devono essere mantenuti in quanto validati dalla fase di monitoraggio e validazione
- trattamenti che hanno consentito di risolvere eventi di sicurezza non previsti dal piano
- eventi di sicurezza, non previsti dal piano precedente

- elenco delle schede di monitoraggio, classificate per minaccia e per attività/processo elementare. Questo costituisce il punto di inizio di un'attività di misura del rischio di tipo quantitativo.

Classificazione e/o aggiornamento del piano versione alfa – classificazione minacce

MACROPROCESSO	PROCESSO	ATTIVITÀ
Titolo del Macroprocesso	Titolo del processo	Descrizione dell'attività
	Nuovo Processo?	Nuova attività?
	☐ SI ☐ NO	☐ SI ☐ NO

Minaccia	Impatto								
	R	I	D	Re	Au	Af	Valore (NBMAC)	Variazione	Commento

In riferimento al nuovo piano di sicurezza, per ogni minaccia e relativa valutazione dell'impatto e, quindi, del rischio, deve essere indicato nella casella "Variazione" lo stato di variazione rispetto al piano di sicurezza precedente. In particolare deve essere riportato una delle seguenti voci:

- *N => Nuova voce non prevista nel piano di sicurezza precedente*
- *M=> Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano*
- *R=>Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano*

Nella casella denominata "Commento" deve essere riportata una nota circa la causa della variazione rispetto al precedente piano di sicurezza.

Classificazione e/o aggiornamento del piano versione alfa – trattamento minacce

MACROPROCESSO Titolo del Macroprocesso		PROCESSO Titolo del processo Nuovo Processo? ☐ SI ☐ NO	ATTIVITÀ Descrizione dell'attività Nuova attività? ☐ SI ☐ NO		
Minaccia	Trattamento scelto	Responsabile	Risorse	Variazione	Commento

In riferimento al nuovo piano di sicurezza, per ogni minaccia e relativa valutazione dell'impatto e, quindi, del rischio, deve essere indicato nel campo "Variazione" lo stato di variazione rispetto al piano di sicurezza precedente. In particolare deve essere riportato uno dei seguenti valori:

- *N -> Nuova voce non prevista nel piano di sicurezza precedente*
- *M-> Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano*
- *R-> Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano*

Nella casella denominata "Commento" deve essere riportata una nota circa la causa della variazione rispetto al precedente piano di sicurezza.

1.4. Variazioni delle procedure operative

Segue il modulo che il Comune è tenuto a consegnare insieme al nuovo Piano di sicurezza per evidenziare le variazioni rispetto al precedente piano circa le procedure operative di riferimento per l'uso e l'emissione della CIE (*allegato "Allegato6-4 ManutenzionaPiano-Variazione procedure operative.doc"*).

Stato Procedure Operative		
Procedure operative	*Variazione*	*Commento*
Procedura di controllo degli accessi		
Procedura di gestione degli account		
Procedura di gestione del materiale in entrata ed in uscita		
Procedura di attivazione dei sistemi comunali		
Procedura di gestione della Quantità di Sicurezza		

Procedura di gestione delle CIE inizializzate		
Procedura di Manutenzione degli apparati		
Procedura di Gestione della rete		
Procedura di Gestione della Porta di accesso ai domini applicativi del CNSD		
Procedura di Gestione delle Postazioni di Emissione		
Procedura di emissione CIE		
Procedura di caricamento dell'INA		
Procedure di attuazione delle norme vigenti sulla sicurezza dell'edificio e del personale		
Procedure operative per la gestione dei eventi straordinari		

L' elenco delle procedure operative deve essere aggiornato rispetto all'elenco delle procedure operative previste sia nel nuovo che nel precedente Piano di sicurezza.

Nella casella "Variazione" deve essere riportato una delle seguenti voci:

- *N=> Nuova voce non prevista nel piano di sicurezza precedente*
- *M=> Voce già definita nel Piano di sicurezza precedente e mantenuta invariata nel nuovo piano*
- *R=> Voce definita nel Piano di sicurezza precedente e rimossa dal nuovo Piano*

Nella casella denominata "Commento" deve essere riportata una nota circa la motivazione della variazione rispetto al precedente piano di sicurezza.

Allegato 7
Documento operativo per i Comuni ai fini della compilazione del piano di sicurezza

1.Introduzione

Il presente allegato presenta il riepilogo finale per la redazione del piano di sicurezza da parte del Comune. Nel seguito è riportato l'indice del piano di sicurezza ed i relativi riferimenti per la definizione dei contenuti.

Il piano di sicurezza ed ogni relativa modifica procedurale che i Comuni intendano introdurre, dovranno essere esplicitamente approvati dalla Prefettura.
Il Comune è tenuto ad inviare il piano di sicurezza alla Prefettura.

Il piano di sicurezza deve essere custodito in sicurezza sia in formato cartaceo che elettronico.
Qualora il piano di sicurezza sia custodito in formato elettronico, deve contenere la data di approvazione della Prefettura e deve essere firmato tramite certificato digitale rilasciato dal Ministero dell'Interno al Comune stesso.

Qualora il piano di sicurezza sia custodito in formato cartaceo, esso deve riportare la data di approvazione della Prefettura e deve essere firmato e vidimato in ogni sua pagina.

Qualsiasi violazione della sicurezza e della riservatezza del Piano di sicurezza stesso deve essere tempestivamente denunciata sia alle autorità competenti, sia alla Prefettura ed al Ministero dell'Interno.

2.Indice Piano di Sicurezza

Di seguito si riporta una tabella riepilogativa che illustra la struttura finale del piano di sicurezza. In relazione ad ogni singolo capitolo del piano di sicurezza, nelle due colonne a destra, sono riportati i riferimenti ai corrispondenti capitoli di questo documento il cui contenuto va interamente trascritto nel piano di sicurezza.

Indice Capitolo	Descrizione Capitolo	Riferimento per i contenuti	
		Documento – capitolo	Descrizione
1	Scopo e campo d'applicazione	Linee guida per la redazione del Piano – Capitolo 1	Scopo e campo di applicazione
2	Riferimenti	Linee guida per la redazione del Piano – Capitolo 2	Riferimenti
3	Definizioni e acronimi	Linee guida per la redazione del Piano – Capitolo 3	Definizioni e acronimi

4	Introduzione	Linee guida per la redazione del Piano – Capitolo 4	Introduzione
		Linee guida per la redazione del Piano – Capitolo 5	Obiettivi
		Linee guida per la redazione del Piano – Capitolo 6	Principi generali
5	Riferimenti normativi e regolamentari	Allegato 1 – Capitolo 1	Descrizione delle norme relative alla sicurezza
6	Politiche di sicurezza e metodologia di attuazione del piano della sicurezza	Allegato 2 – Capitolo 1	Ambito di applicazione del Piano della Sicurezza Comunale
		Allegato 2 – Capitolo 2	Attuazione del Piano della Sicurezza Comunale
		Allegato 2 – Capitolo 3	Politiche di sicurezza
		Linee guida per la redazione del Piano – Capitolo 8	Metodologia utilizzata
7	Descrizione struttura tecnica, logistica ed organizzativa del Comune	Allegato 3- capitolo 3	Struttura generale, modalità organizzativa e struttura logistica di riferimento per l'emissione e l'uso della CIE
8	Procedure e relativi flussi informativi di emissione ed uso della CIE	Allegato 3 - capitolo 4	Macroprocessi e relativi flussi informativi di emissione ed uso CIE
		Allegato 4 - capitolo 7	Definizione delle procedure operative
9	Classificazione delle minacce e delle vulnerabilità ai fini della valutazione del rischio	Allegato 4 – Capitolo 2	Schede di classificazione delle minacce e delle vulnerabilità
		Allegato 4 – capitolo 3	Minacce e vulnerabilità
		Allegato 5 – capitolo 4	Valutazione del rischio
		Allegato 4 – capitolo 5	Trattamento del rischio
		Allegato 4 – capitolo 6	Attuazione dei trattamenti
10	Monitoraggio del	Allegato 5 –	Schede di monitoraggio e validazione

	Piano	capitolo 2	del Piano di Sicurezza
11	Manutenzione ed evoluzione del piano	Allegato 6 – capitolo 1	Descrizione delle attività
12	Allegati	N/A	Riportare l'elenco di tutti gli allegati. Tra gli allegati devono essere riportate tutte le schede compilate per la stesura del Piano di Sicurezza

Rispetto all'indice descritto si evidenzia:

- capitoli da 1 a 6:
  - i contenuti riportati nei riferimenti indicati sono considerati esaustivi.
- capitoli da 7 a 9: i contenuti riportati nei riferimenti indicati sono considerati esaustivi. Il Comune è tenuto alla compilazione di tutte le schede.
- capitoli 10 e 11: i contenuti riportati nei riferimenti indicati sono considerati esaustivi.
- capitolo 12: il Comune è tenuto ad elencare tutti gli allegati al Piano di Sicurezza. Ricordiamo che il Comune è tenuto a fornire anche le seguenti informazioni:
  - Descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza CIE
  - Ubicazione dei servizi e degli uffici CIE negli immobili
  - Elenco del personale e sua assegnazione agli uffici.

ALLEGATO B
REGOLE TECNICHE E DI SICUREZZA
PER L'ACCESSO AI DOMINI APPLICATIVI DEL CNSD

INDICE

1. Introduzione

Tutti gli accessi ai servizi INA ed ai servizi di emissione ed uso della CIE, avvengono nell'ambito delle seguenti infrastrutture di sicurezza:

- Porta di accesso ai domini applicativi del CNSD ("Porta di accesso") : la Porta di accesso, attraverso il Backbone CNSD, ai servizi del C.N.S.D. secondo standard "busta di e-gov" di SPC
- Backbone di Sicurezza del CNSD ("Backbone"): la dorsale di sicurezza e certificazione del CNSD per l'accesso ai servizi applicativi del CNSD;
- SSCE: Sistema di Sicurezza del Circuito di Emissione delle carte di identità e dei documenti di identità elettronici.
- Modello asincrono di emissione CIE

In conformità con le infrastrutture di sicurezza sopra elencate, nel rispetto della normativa anagrafica e delle prerogative del Ministero dell'Interno per quanto riguarda la vigilanza anagrafica, per gli accessi ai domini applicativi del CNSD è previsto:

- *Porta di accesso ai domini applicativi del CNSD*: ogni porta di accesso ai domini applicativi del CNSD è identificata in modo univoco ed è associata in modo certo e sicuro al Comune. La Porta di accesso del comune identifica il punto di accesso autorizzato, presente presso la struttura comunale, che consente la fruizione in sicurezza dei servizi erogati dal CNSD stesso. La Porta di accesso certifica quindi il punto di origine delle comunicazioni, individuando univocamente il Comune che, tramite la Porta di accesso, si collega al CNSD. Nessuna altra modalità di comunicazione è quindi possibile tra comune e CNSD.
- *abilitazione dei sistemi comunali per l'accesso ai domini applicativi del CNSD*: ogni sistema comunale che deve accedere ai domini applicativi del CNSD, deve essere abilitato presso la Porta di accesso ai domini applicativi del CNSD, al fine di assicurare l'accesso ai domini applicativi del CNSD dai soli sistemi comunali abilitati. I sistemi comunali abilitati all'accesso ai domini applicativi del CNSD, sono identificati in modo certo e sicuro da appositi certificati di abilitazione.
- *documentazione e certificazione degli accessi ai domini applicativi del CNSD*: monitoraggio degli accessi ai domini applicativi al fine di fornire in modo preciso ed inequivocabile tutte le informazioni necessarie a descrivere l'evento e ad individuare le responsabilità;
- *rilevazione, controllo e gestione degli allarmi*: rilevazione, controllo e gestione degli allarmi inerenti accessi ed usi impropri dei domini applicativi del CNSD.

Gli ultimi due punti , "*documentazione e certificazione degli accessi ai domini applicativi del CNSD*" e "*rilevazione, controllo e gestione degli allarmi*" sono servizi di supporto per le funzionalità di CERT (*Computer Emergency Response Team, ovvero* "Unità di gestione degli attacchi informatici").

I livelli di sicurezza relativi ai sistemi ed ai prodotti per il circuito di emissione CIE e per la Porta di accesso ai domini applicativi del CNSD, sono certificati dal Ministero dell'Interno-CNSD.

Il CNSD rende disponibili attraverso la Porta di accesso ai domini applicativi del CNSD, servizi di sicurezza per l'accesso ai sistemi distribuiti di verifica dello stato dei certificati CIE e dei certificati di abilitazione dei sistemi comunali.

Nel seguito sono riportate le specifiche tecniche di riferimento per l'accesso ai domini applicativi del CNSD. In particolare le specifiche tecniche si riferiscono a:

- Attivazione Porta di accesso ai domini applicativi del CNSD
- Accesso al dominio applicativo INA del CNSD
- Accesso al dominio applicativo CIE del CNSD

2. Attivazione Porta di accesso ai domini applicativi del CNSD

La porta di accesso ai domini applicativi del CNSD, denominata anche porta di dominio del CNSD, è l'unico punto autorizzato per l'accesso al CNSD stesso.
Ogni porta di accesso ai domini applicativi del CNSD è identificata in modo univoco ed è associata in modo certo al comune.

Tutti i flussi verso il CNSD devono passare per la Porta di accesso ai domini applicativi del CNSD, non sono consentite altre modalità di comunicazione con il CNSD.

La Porta di accesso ai domini applicativi del CNSD per essere attivata e, quindi, per essere operativa, deve essere registrata presso il CNSD che concedere le relative autorizzazioni.

Per l'attivazione della Porta di accesso ai domini al CNSD è indispensabile che il Comune abbia acquisito dal Ministero le "*quantità di sicurezza, attivazione e certificazione*".
Le "*quantità di sicurezza, attivazione e certificazione*" rappresentano il supporto tecnologico-informatico fornito dal Ministero al Comune. Tale supporto contiene i seguenti elementi:

- strumenti di sicurezza (agenti di controllo monitoraggio e allarme, certificati digitali, dotazioni di servizio) richiesti per l'attivazione della Porta di accesso ai domini applicativi del CNSD e per l'attivazione dei sistemi comunali autorizzati all'accesso ai domini applicativi del CNSD.

I certificati digitali resi disponibili nelle "*quantità di sicurezza, attivazione e certificazione*" sono rilasciati dalla CA (Certification Authority) istituita presso il CNSD.

Una volta predisposti i sistemi hardware e software di base ed a segúito della corretta configurazione della rete, per l'attivazione della Porta di accesso ai domini applicativi del CNSD sono necessarie:

a. Abilitazione della porta: tramite il supporto tecnologico-informatico "*quantità di sicurezza, attivazione e certificazione*" rilasciato al Comune dal Ministero, sulla postazione sono installati i seguenti moduli software:
    - Modulo Backbone e Porta di accesso ai domini applicativi del CNSD
    - Agente di monitoraggio
    - Agente di controllo e rilevazione allarmi.
    - certificato digitale server per il colloquio secondo standard SSL

b. Registrazione della Porta di acceso ai domini applicativi del CNSD tramite "quantità di sicurezza, attivazione e certificazione".

c. Prova del corretto funzionamento della Porta di accesso ai domini applicativi del CNSD in termini di sicurezza e di dimensionamento dei flussi di comunicazione

d. Certificazione della porta di accesso ai domini applicativi del CNSD in funzione dei risultati della prova di corretto funzionamento di cui al punto c.

Al termine delle quattro fasi sopra descritte, la porta si ritiene attivata e, quindi, è ritenuta un punto di accesso al CNSD riconosciuto ed autorizzato per il Comune.

Qualsiasi modifica della rete o delle abilitazioni di accesso, deve essere preventivamente comunicata al Ministero dell'Interno che si riserva di verificarne la conformità rispetto alle regole di sicurezza per l'accesso ai domini applicativi del CNSD.

Nei sottoparagrafi seguenti sono descritte le specifiche tecniche relative a :

- Requisiti hardware e software di base
- Requisiti di connettività verso il CNSD della porta di accesso ai domini applicativi del CNSD.

2.1. *Requisiti hardware e software di base*

Il sistema che ospita la porta di accesso ai domini applicativi del CNSD, deve soddisfare i seguenti requisiti minimi:

- Processore Pentium IV o compatibile (1,3 Ghz di clock)
- 512 Mb di RAM
- 40 Gb di HD
- Scheda di rete Ethernet 10/100

Per la Porta di accesso ai domini applicativi del CNSD i sistemi operativi compatibili sono:

- Sistemi Operativi Microsoft:
    - Windows 2000 Professional/Server (si ricorda che la Microsoft ha recentemente dichiarato che non sono previste ulteriori attività di manutenzione e di soluzione di problemi di sicurezza per i sistemi operativi Windows 2000. Quindi i comuni che dovessero acquisire ex novo un sistema operativo per la porta di accesso ai domini applicativi del CNSD non devono acquisire tale sistema operativo Windows 2000)

- o Windows XP Professional Edition
    - o Windows Server 2003
- Sistema Operativo Linux:
    - o Versione Kernel 2.4.1 o superiore

2.2. *Requisiti di connettività della Porta di accesso ai domini applicativi del CNSD*

Per le comunicazioni che transitano verso i domini applicativi del CNSD, la porta di accesso e tutti gli apparati di rete interessati dai flussi da e verso la Porta di accesso devono rispettare le regole di sicurezza riportate nella tabella seguente.

Regole di connettività richieste per la comunicazione tra Porta di accesso ai domini applicativi del CNSD presso il Comune e il CNSD stesso

Dominio applicativo del CNSD	**Indirizzi IP Remoti**		**Nome HOST**	**Porte TCP**	**Protocollo**	**Descrizione flussl**
	Accesso da Internet	**Accesso da RUPA INTERDOMINIO**				
Infrastruttura di sicurezza Backbone				80 389 443 2560 7001 7002 8080 8081 8082 8083 8084 8090 8091	TCP/IP	Servizi di gestione dell'infrastruttura di sicurezza backbone e di registrazione delle Porte di accesso ai domini applicativi del CNSD installate presso i comuni
Servizi di monitoraggio, rilevazione e controllo allarmi	80.207.109.110 160.80.212.82 80.207.109.105 80.207.109.124	80.253.38.140 80.253.38.163 80.253.38.135 80.253.38.154 80.253.38.149	controllo.cnsd.interno.it www.conformita.it soap.cnsd.interno.it			Servizi per il controllo e la certificazione dello stato di funzionamento ed operatività sia della postazione di emissione CIE, sia delle Porte di accesso ai domini applicativi del CNSD.
Dominio Applicativo Servizi Anagrafici	80.207.109.119 80.207.109.121 80.207.109.122 80.207.109.123	80.253.38.151 80.253.38.152 80.253.38.153				Servizi applicativi anagrafici (servizi INA). Il flusso di comunicazione è basato su busta e-gov con protocollo SOAP, secondo lo standard CNIPA (http://www.cnipa.gov.it/site/_files/4.SPC_Busta%20e-Gov%20v.1_0-21-04-2004.pdf).
Dominio Applicativo						

Dominio applicativo del CNSD	**Indirizzi IP Remoti**		**Nome HOST**	**Porte TCP**	**Protocollo**	**Descrizione flussi**
	Accesso da Internet	**Accesso da RUPA INTERDOMINIO**				
Servizi di emissione CIE						Tutti i flussi sono trasmessi su canale sicuro tramite infrastruttura di sicurezza Backbone. Servizi applicativi di emissione CIE. Tutti i flussi sono trasmessi in modalità sicura tramite infrastruttura del sistema di sicurezza del Circuito di Emissione delle carte d'identità e dei documenti d'identità elettronici.

Per tutte le comunicazioni indicate, non deve essere impostato alcun tipo di filtro sugli apparati di rete intermedi e la comunicazione deve avvenire in assenza di proxy http intermedi.

3. Accesso al dominio applicativo INA del CNSD

Tutti i servizi INA del CNSD (dominio applicativo INA) sono erogati nell'ambito dell'infrastruttura di sicurezza Backbone di Sicurezza del CNSD e Porta comunale di accesso ai domini applicativi del CNSD.

I sistemi applicativi comunali devono comunicare con la Porta di accesso ai domini applicativi del CNSD in una delle seguenti modalità:

- Post XML su protocollo http
- Protocollo XML SOAP secondo le specifiche del Sistema Pubblico di Connettività (Busta SPCoop, estensione standard di SOAP 1.1)

La Porta di accesso ai servizi applicativi del CNSD, a sua volta,verifica la conformità dei flussi informativi, predispone la "*busta e-gov*" secondo le specifiche del Sistema Pubblico di Connettività (Busta SPCoop, estensione standard di SOAP 1.1) ed invia la stessa al CNSD gestendo tutte le credenziali di sicurezza relative all'infrastruttura Backbone.

Si ricorda che solo i sistemi comunali registrati presso la porta di accesso ai domini applicativi del CNSD sono autorizzati all'accesso ai domini applicativi del CNSD stesso.

La procedura di attivazione di un sistema comunale per l'accesso ai servizi del dominio applicativo INA del CNSD richiede:

- *Abilitazione del sistema comunale per l'accesso al dominio applicativo INA*: tramite il supporto tecnologico-informatico "*quantità di sicurezza, attivazione e certificazione*" rilasciato al Comune dal Ministero, sulla postazione sono installati i seguenti moduli di sicurezza:
  - modulo di registrazione del sistema presso la porta di accesso ai domini applicativi del CNSD: dal supporto tecnologico-informatico, fornito dal Ministero dell'Interno vengono scaricati sul sistema comunale i certificati digitali client forniti per l'abilitazione alla comunicazione, secondo standard SSL, del sistema comunale stesso con la Porta di accesso.
  - Modulo di verifica della sicurezza e della connettività tra sistema comunale e Porta di accesso

- *Registrazione del sistema alla Porta di accesso ai domini applicativi del CNSD*: il modulo di registrazione, attivato solo ed esclusivamente in presenza della "*quantità di sicurezza, attivazione e certificazione*", consente di autorizzare il sistema presso la Porta di accesso ai domini applicativi del CNSD, abilitandolo all'accesso al dominio applicativo INA del CNSD
- *Test per la corretta configurazione della sicurezza e dei canali di comunicazione*: il modulo software di test della sicurezza e della connettività consente di verificare la corretta configurazione delle impostazioni di rete così come indicate nel sottoparagrafo successivo. L'attivazione può proseguire solo a seguito dell'esito positivo dei test.
- *Attivazione finale del sistema per l'accesso al dominio applicativo INA del CNSD*: il sistema è attivato per l'accesso, tramite Porta di accesso ai domini applicativi del CNSD, ai servizi INA del CNSD. Presso il sistema, in presenza sempre delle "*quantità di sicurezza, attivazione e certificazione*", sono rilasciati i certificati digitali per l'abilitazione all'accesso ai servizi INA del CNSD.

Al termine delle fasi sopra descritte, il sistema è attivato e, quindi, è autorizzato ad inviare le informazioni (attraverso il protocollo XML SOAP o Post XML) alla Porta di accesso che, creata la "*busta di e-gov*", la trasmette tramite Backbone al CNSD per l'accesso al servizio per cui è stata effettuata l'attivazione.

Qualsiasi modifica della rete o delle abilitazioni di accesso, deve essere preventivamente comunicata al Ministero dell'Interno che si riserva di verificarne la conformità rispetto alle regole di sicurezza per l'accesso ai domini applicativi del CNSD.

Nel sottoparagrafo successivo sono riportati i requisiti di connettività tra sistema comunale e Porta di accesso ai domini applicativi del CNSD.

3.1. *Accesso al dominio applicativo INA del CNSD - Requisiti di connettività tra sistemi comunali e Porta di accesso ai domini applicativi del CNSD*

Per le comunicazioni con la Porta di accesso ai domini applicativi del CNSD, i sistemi comunali abilitati all'accesso ai servizi INA del CNSD e tutti i sistemi di rete intermedi, devono rispettare le regole di sicurezza e di connettività riportate nella tabella seguente.

Si noti che gli indirizzi IP non sono riportati in quanto, a livello di rete comunale, è responsabilità del Comune assegnare gli indirizzi IP agli apparati installati presso la propria rete.
Si evidenzia che l'architettura è compatibile rispetto all'integrazione con le reti regionali.

Accesso ai servizi INA del CNSD - Tabella regole di connettività richieste per la comunicazione tra sistema comunale e Porta di accesso ai domini applicativi del CNSD

Servizio	**Porte TCP**	**Protocollo**	**Descrizione flusso**
Registrazione Sistema comunale Accesso ai servizi INA del CNSD tramite Post XML su protocollo HTTP Accesso ai servizi INA del CNSD tramite protocollo XML SOAP	60000 60001 80 443 8080	TCP/IP	Attivazione del sistema comunale all'accesso al dominio applicativo INA del CNSD Post XML su protocollo http Protocollo SOAP

Per tutte le comunicazioni indicate, non deve essere impostato alcun tipo di filtro sugli apparati di rete intermedi e la comunicazione deve avvenire in assenza di proxy http intermedi.

4. Accesso al dominio applicativo CIE del CNSD

Tutti i servizi CIE del CNSD sono erogati nell'ambito del Sistema di Sicurezza del Circuito di Emissione delle carte di identità e dei documenti di identità elettronici.

Nell'ambito del Sistema di Sicurezza del Circuito di Emissione delle carte di identità e dei documenti di identità elettronici, le comunicazioni tra infrastruttura comunale e CNSD sono gestite, sempre tramite la Porta di accesso ai domini applicativi del CNSD, dal *punto di back office* per la comunicazione con il dominio applicativo CIE.

Analogamente a quanto già richiesto per i sistemi comunali per l'accesso al dominio applicativo INA, anche per le postazioni di emissione CIE è richiesta la procedura di attivazione per l'accesso al dominio applicativo CIE. La procedura prevede:

- *Abilitazione delle postazioni di emissione CIE*: tramite il supporto tecnologico-informatico "*quantità di sicurezza, attivazione e certificazione*" rilasciato al Comune di riferimento dal Ministero, sulla postazione sono installati i seguenti moduli software:
    - modulo di registrazione del sistema presso la porta di accesso ai domini applicativi del CNSD;
    - Agenti di monitoraggio
    - Agenti di controllo e rilevazione degli allarmi
    - Modulo di test della connettività
- *Registrazione del sistema alla Porta comunale di accesso ai domini applicativi del CNSD*: il modulo di registrazione, attivato solo ed esclusivamente in presenza della "*quantità di sicurezza, attivazione e certificazione*", consente di autorizzare presso la Porta di accesso ai domini applicativi del CNSD le postazioni CIE abilitandole all'accesso al dominio applicativo CIE del CNSD.
- *Installazione e attivazione del software di emissione CIE.*
- *Test per la corretta configurazione della sicurezza e dei canali di comunicazione*: il modulo software di verifica della sicurezza e della connettività consente di verificare la corretta configurazione delle impostazioni di rete così come indicate nel sottoparagrafo successivo. L'attivazione può proseguire solo a seguito dell'esito positivo dei test.
- *Attivazione finale del sistema per l'accesso al dominio applicativo CIE*: il sistema è attivato per l'accesso tramite Porta di accesso ai domini applicativi del CNSD, ai servizi centrali di emissione CIE.

Al termine delle fasi sopra descritte, il sistema si ritiene attivato e, quindi, è autorizzato ad inviare le informazioni alla Porta di accesso che le trasmette presso il CNSD al servizio di emissione CIE.

Si evidenzia che a differenza dei sistemi comunali attivati per l'accesso ai domini applicativi del CNSD, per le postazioni di emissione CIE, a seguito dell'attivazione, non sono assegnati certificati digitali di abilitazione. In questo caso, i certificati digitali di abilitazione non sono richiesti in quanto il software di emissione CIE, a differenza del software che può essere usato dai comuni per la gestione degli altri servizi, è un software rilasciato direttamente dal Ministero ed ha i propri certificati di abilitazione.

Qualsiasi modifica della rete o delle abilitazioni di accesso, deve essere preventivamente comunicata al Ministero dell'Interno che si riserva di verificarne la conformità rispetto alle regole di sicurezza per l'accesso ai domini applicativi del CNSD.

Nel sottoparagrafo successivo sono riportati i requisiti di sicurezza e di connettività tra sistema CIE presso i comuni e la Porta di accesso ai domini applicativi del CNSD.

Per le caratteristiche hardware e software delle postazioni di emissione, si rimanda alla documentazione di riferimento acquisibile presso il sito del CNSD, area CIE.

4.1. *Accesso al dominio applicativo CIE del CNSD - Requisiti di sicurezza e connettività tra sistemi CIE e Porta di accesso ai domini applicativi del CNSD*

Per le comunicazioni con la Porta di accesso ai domini applicativi del CNSD, i sistemi di emissione CIE del Comune (postazioni CIE di front office e di back office) abilitati all'accesso ai domini applicativi del CNSD e tutti i sistemi di rete intermedi, devono rispettare le regole di connettività riportate nella tabella seguente.
Si noti che gli indirizzi IP non sono riportati in quanto, a livello di rete comunale, è responsabilità del Comune assegnare gli indirizzi IP agli apparati installati presso la propria rete.

Accesso al dominio applicativo CIE del CNSD - Tabella regole di connettività richieste per la comunicazione tra sistema comunale e Porta di accesso ai domini applicativi del CNSD

Servizio	Porte TCP	Protocollo	Descrizione flusso
Registrazione Sistema comunale Flussi degli agenti di monitoraggio, controllo e rilevazione degli allarmi Accesso ai servizi CIE	389 2560 7001 7002 8081 8082 8083 8084 8090 8091 7003 7004 7005 7006 60000 60001	TCP/IP	Servizi per l'attivazione, a livello di rete comunale, dell'accesso al dominio applicativo CIE del CNSD Servizi per il controllo e la certificazione dello stato di funzionamento ed operatività sia delle postazioni di emissione CIE, sia della Porta di accesso ai domini applicativi del CNSD. Servizi CIE

Per tutte le comunicazioni indicate, non deve essere impostato alcun tipo di filtro sugli apparati di rete intermedi e la comunicazione deve avvenire in assenza di proxy http intermedi.

05A08041

AUGUSTA IANNINI, *direttore* FRANCESCO NOCITA, *redattore*

(G503123/1) Roma, 2005 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE

cap	località	libreria	indirizzo	pref.	tel.	fax
95024	**ACIREALE (CT)**	CARTOLIBRERIA LEGISLATIVA S.G.C. ESSEGICI	Via Caronda, 8-10	095	7647982	7647982
00041	**ALBANO LAZIALE (RM)**	LIBRERIA CARACUZZO	Corso Matteotti, 201	06	9320073	93260286
60121	**ANCONA**	LIBRERIA FOGOLA	Piazza Cavour, 4-5-6	071	2074606	2060205
83100	**AVELLINO**	LIBRERIA PIROLA MAGGIOLI	Via Matteotti, 30/32	0825	30597	248957
81031	**AVERSA (CE)**	LIBRERIA CLA.ROS	Via L. Da Vinci, 18	081	8902431	8902431
70124	**BARI**	CARTOLIBRERIA QUINTILIANO	Via Arcidiacono Giovanni, 9	080	5042665	5610818
70121	**BARI**	LIBRERIA UNIVERSITÀ E PROFESSIONI	Via Crisanzio, 16	080	5212142	5243613
13900	**BIELLA**	LIBRERIA GIOVANNACCI	Via Italia, 14	015	2522313	34983
40132	**BOLOGNA**	LIBRERIA GIURIDICA EDINFORM	Via Ercole Nani, 2/A	051	4218740	4210565
40124	**BOLOGNA**	LIBRERIA GIURIDICA - LE NOVITÀ DEL DIRITTO	Via delle Tovaglie, 35/A	051	3399048	3394340
21052	**BUSTO ARSIZIO (VA)**	CARTOLIBRERIA CENTRALE BORAGNO	Via Milano, 4	0331	626752	626752
91022	**CASTELVETRANO (TP)**	CARTOLIBRERIA MAROTTA & CALIA	Via Q. Sella, 106/108	0924	45714	45714
95128	**CATANIA**	CARTOLIBRERIA LEGISLATIVA S.G.C. ESSEGICI	Via F. Riso, 56/60	095	430590	508529
88100	**CATANZARO**	LIBRERIA NISTICÒ	Via A. Daniele, 27	0961	725811	725811
66100	**CHIETI**	LIBRERIA PIROLA MAGGIOLI	Via Asinio Herio, 21	0871	330261	322070
22100	**COMO**	LIBRERIA GIURIDICA BERNASCONI - DECA	Via Mentana, 15	031	262324	262324
87100	**COSENZA**	LIBRERIA DOMUS	Via Monte Santo, 70/A	0984	23110	23110
50129	**FIRENZE**	LIBRERIA PIROLA già ETRURIA	Via Cavour 44-46/R	055	2396320	288909
71100	**FOGGIA**	LIBRERIA PATIERNO	Via Dante, 21	0881	722064	722064
03100	**FROSINONE**	L'EDICOLA	Via Tiburtina, 224	0775	270161	270161
16121	**GENOVA**	LIBRERIA GIURIDICA	Galleria E. Martino, 9	010	565178	5705693
95014	**GIARRE (CT)**	LIBRERIA LA SEÑORITA	Via Trieste angolo Corso Europa	095	7799877	7799877
73100	**LECCE**	LIBRERIA LECCE SPAZIO VIVO	Via Palmieri, 30	0832	241131	303057
74015	**MARTINA FRANCA (TA)**	TUTTOUFFICIO	Via C. Battisti, 14/20	080	4839784	4839785
98122	**MESSINA**	LIBRERIA PIROLA MESSINA	Corso Cavour, 55	090	710487	662174
20100	**MILANO**	LIBRERIA CONCESSIONARIA I.P.Z.S.	Galleria Vitt. Emanuele II, 11/15	02	865236	863684
70056	**MOLFETTA (BA)**	LIBRERIA IL GHIGNO	Via Salepico, 47	080	3971365	3971365

Segue: **LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE**

cap	**località**	libreria	indirizzo	pref.	tel.	fax
80139	**NAPOLI**	LIBRERIA MAJOLO PAOLO	Via C. Muzy, 7	081	282543	269898
80134	**NAPOLI**	LIBRERIA LEGISLATIVA MAJOLO	Via Tommaso Caravita, 30	081	5800765	5521954
28100	**NOVARA**	EDIZIONI PIROLA E MODULISTICA	Via Costa, 32/34	0321	626764	626764
90138	**PALERMO**	LA LIBRERIA DEL TRIBUNALE	P.za V.E. Orlando, 44/45	091	6118225	552172
90138	**PALERMO**	LIBRERIA S.F. FLACCOVIO	Piazza E. Orlando, 15/19	091	334323	6112750
90145	**PALERMO**	LIBRERIA COMMISSIONARIA G. CICALA INGUAGGIATO	Via Galileo Galilei, 9	091	6828169	6822577
90133	**PALERMO**	LIBRERIA FORENSE	Via Maqueda, 185	091	6168475	6177342
43100	**PARMA**	LIBRERIA MAIOLI	Via Farini, 34/D	0521	286226	284922
06087	**PERUGIA**	CALZETTI & MARIUCCI	Via della Valtiera, 229	075	5997736	5990120
29100	**PIACENZA**	NUOVA TIPOGRAFIA DEL MAINO	Via Quattro Novembre, 160	0523	452342	461203
59100	**PRATO**	LIBRERIA CARTOLERIA GORI	Via Ricasoli, 26	0574	22061	610353
00192	**ROMA**	LIBRERIA DE MIRANDA	Viale G. Cesare, 51/E/F/G	06	3213303	3216695
00195	**ROMA**	COMMISSIONARIA CIAMPI	Viale Carso, 55-57	06	37514396	37353442
00161	**ROMA**	L'UNIVERSITARIA	Viale Ippocrate, 99	06	4441229	4450613
00187	**ROMA**	LIBRERIA GODEL	Via Poli, 46	06	6798716	6790331
00187	**ROMA**	STAMPERIA REALE DI ROMA	Via Due Macelli, 12	06	6793268	69940034
45100	**ROVIGO**	CARTOLIBRERIA PAVANELLO	Piazza Vittorio Emanuele, 2	0425	24056	24056
63039	**SAN BENEDETTO D/T (AP)**	LIBRERIA LA BIBLIOFILA	Via Ugo Bassi, 38	0735	587513	576134
07100	**SASSARI**	MESSAGGERIE SARDE LIBRI & COSE	Piazza Castello, 11	079	230028	238183
10122	**TORINO**	LIBRERIA GIURIDICA	Via S. Agostino, 8	011	4367076	4367076
21100	**VARESE**	LIBRERIA PIROLA	Via Albuzzi, 8	0332	231386	830762
36100	**VICENZA**	LIBRERIA GALLA 1880	Viale Roma, 14	0444	225225	225238

MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni dell'Istituto sono in vendita al pubblico:

- **presso l'Agenzia dell'Istituto Poligrafico e Zecca dello Stato S.p.A. in ROMA, piazza G. Verdi, 10 - ☎ 06 85082147;**
- **presso le librerie concessionarie indicate (elenco consultabile sul sito www.ipzs.it)**

L'Istituto conserva per la vendita le Gazzette degli ultimi 4 anni fino ad esaurimento. Le richieste per corrispondenza potranno essere inviate a:

Funzione Editoria - U.O. DISTRIBUZIONE
Attività Librerie concessionarie, Vendita diretta e Abbonamenti a periodici
Piazza Verdi 10, 00198 Roma
fax: 06-8508-4117
e-mail: editoriale@ipzs.it

avendo cura di specificare nell'ordine, oltre al fascicolo di GU richiesto, l'indirizzo di spedizione e di fatturazione (se diverso) ed indicando il codice fiscale per i privati. L'importo della fornitura, maggiorato di un contributo per le spese di spedizione, sarà versato in contanti alla ricezione.

Le inserzioni, come da norme riportate nella testata della parte seconda, si ricevono con pagamento anticipato, presso le agenzie in Roma e presso le librerie concessionarie.

Per informazioni, prenotazioni o reclami attinenti agli abbonamenti oppure alla vendita della *Gazzetta Ufficiale* bisogna rivolgersi direttamente all'Amministrazione, presso l'Istituto Poligrafico e Zecca dello Stato - Piazza G. Verdi, 10 - 00100 ROMA

Gazzetta Ufficiale Abbonamenti	Vendite	Ufficio inserzioni	Numero verde
☎ 800-864035 - Fax 06-85082520	☎ 800-864035 - Fax 06-85084117	☎ 800-864035 - Fax 06-85082242	☎ 800-864035

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

CANONI DI ABBONAMENTO ANNO 2005 (salvo conguaglio) (*)

Ministero dell'Economia e delle Finanze - *Decreto 24 dicembre 2003* (G.U. *n. 36 del 13 febbraio 2004)*

GAZZETTA UFFICIALE - PARTE I (legislativa)

		CANONE DI ABBONAMENTO	
Tipo A	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:		
	(di cui spese di spedizione € 219,04)	- annuale	€ **400,00**
	(di cui spese di spedizione € 109,52)	- semestrale	€ **220,00**
Tipo A1	Abbonamento ai fascicoli della serie generale, inclusi i soli supplementi ordinari contenenti i provvedimenti legislativi:		
	(di cui spese di spedizione € 108,57)	- annuale	€ **285,00**
	(di cui spese di spedizione € 54,28)	- semestrale	€ **155,00**
Tipo B	Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale:		
	(di cui spese di spedizione € 19,29)	- annuale	€ **68,00**
	(di cui spese di spedizione € 9,64)	- semestrale	€ **43,00**
Tipo C	Abbonamento ai fascicoli della serie speciale destinata agli atti della CE:		
	(di cui spese di spedizione € 41,27)	- annuale	€ **168,00**
	(di cui spese di spedizione € 20,63)	- semestrale	€ **91,00**
Tipo D	Abbonamento ai fascicoli della serie destinata alle leggi e regolamenti regionali:		
	(di cui spese di spedizione € 15,31)	- annuale	€ **65,00**
	(di cui spese di spedizione € 7,65)	- semestrale	€ **40,00**
Tipo E	Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:		
	(di cui spese di spedizione € 50,02)	- annuale	€ **167,00**
	(di cui spese di spedizione € 25,01)	- semestrale	€ **90,00**
Tipo F	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari, ed ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 344,93)	- annuale	€ **780,00**
	(di cui spese di spedizione € 172,46)	- semestrale	€ **412,00**
Tipo F1	Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari con i provvedimenti legislativi e ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 234,45)	- annuale	€ **652,00**
	(di cui spese di spedizione € 117,22)	- semestrale	€ **342,00**

N.B.: L'abbonamento alla GURI tipo A, A1, F, F1 comprende gli indici mensili
Integrando con la somma di € **80,00** *il versamento relativo al tipo di abbonamento alla* Gazzetta Ufficiale - *parte prima - prescelto, si riceverà anche l'Indice Repertorio Annuale Cronologico per materie anno 2005.*

BOLLETTINO DELLE ESTRAZIONI

Abbonamento annuo (incluse spese di spedizione) € **88,00**

CONTO RIASSUNTIVO DEL TESORO

Abbonamento annuo (incluse spese di spedizione) € **56,00**

PREZZI DI VENDITA A FASCICOLI

(Oltre le spese di spedizione)

Prezzi di vendita:		
	serie generale	€ 1,00
	serie speciali (escluso concorsi), ogni 16 pagine o frazione	€ 1,00
	fascicolo serie speciale, *concorsi,* prezzo unico	€ 1,50
	supplementi (ordinari e straordinari), ogni 16 pagine o frazione	€ 1,00
	fascicolo Bollettino Estrazioni, ogni 16 pagine o frazione	€ 1,00
	fascicolo Conto Riassuntivo del Tesoro, prezzo unico	€ 6,00

I.V.A. 4% a carico dell'Editore

GAZZETTA UFFICIALE - PARTE II (inserzioni)

Abbonamento annuo	*(di cui spese di spedizione € 120,00)*		€ **320,00**
Abbonamento semestrale	*(di cui spese di spedizione € 60,00)*		€ **185,00**
Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione)		€ 1,00	

I.V.A. 20% inclusa

RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI

Abbonamento annuo		€ **190,00**
Abbonamento annuo per regioni, province e comuni		€ **180,00**
Volume separato (oltre le spese di spedizione)	€ 18,00	

I.V.A. 4% a carico dell'Editore

Per l'estero i prezzi di vendita, in abbonamento ed a fascicoli separati, anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso. Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli, vengono stabilite, di volta in volta, in base alle copie richieste.

N.B. - Gli abbonamenti annui decorrono dal 1° gennaio al 31 dicembre, i semestrali dal 1° gennaio al 30 giugno e dal 1° luglio al 31 dicembre.

Restano confermati gli sconti in uso applicati ai soli costi di abbonamento

ABBONAMENTI UFFICI STATALI

Resta confermata la riduzione del 52% applicata sul solo costo di abbonamento

* tariffe postali di cui al Decreto 13 novembre 2002 (G.U. n. 289/2002) e D.P.C.M. 27 novembre 2002 n. 294 (G.U. 1/2003) per soggetti iscritti al R.O.C.